No. 156 Julio - Septiembre 2020 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2017-186 4-72, vence 31 de Dic. 2020

EDGE COMPUTING

Computación en el borde y en la niebla

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

Propuesta de valor

globaltek SECURITY

25+ AÑOS

SERVICIO ADMINISTRADO DE CIBERSEGURIDAD BASADO EN RIESGOS

Globaltek Security le ayuda a identificar, detectar, categorizar, responder a las amenazas de la red, responder al punto final en el trabajo remoto, a contener, remediar y actualizar el mapa de riesgos incluyendo riesgos emergentes.

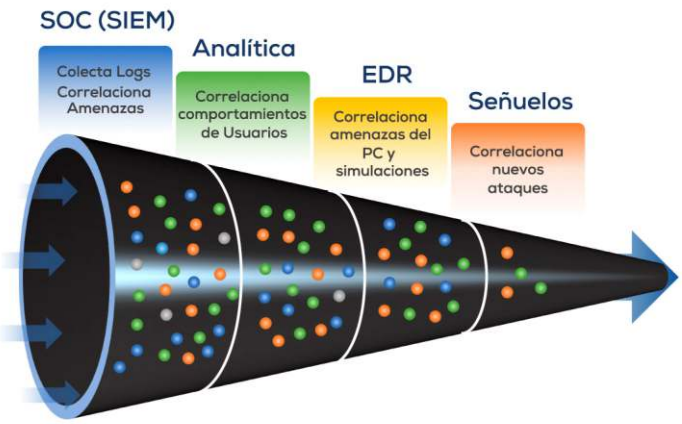
Simular Nuevas Amenazas: APT

Analizar Amenazas actuales: NGFW, DLP, Antimalware, Antiransomware

Riesgos Emergentes: Analítica del comportamiento de los Usuarios

Cazar amenazas: EDR y Señuelos [*]

Correlación de Amenazas: SIEM [*]



Gestión de incidentes mediante consola **RPA + IA + Analítica** evaluando el comportamiento del adversario

[*] Servicio básico

Analizar Riesgos Conocidos: Análisis de vulnerabilidades de activos sensibles y generación de políticas basadas en riesgos [*]

¡CONTÁCTANOS!

comercial@globalteksecurity.com | **(+57 1) 310 232 1344**

Síguenos en:

Globaltek Security

Más información:

www.**globalteksecurity**.com

En esta edición

Publicación de la Asociación Colombiana de
Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del
Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales
Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Dirección General
Jeimy J. Cano Martínez

Consejo de Redacción
Francisco Rueda F.
Gabriela Sánchez A.
Manuel Dávila S.
Andrés Ricardo Almanza J.
Emir Hernando Pernet C.
Fabio Augusto González O.
Jorge Eliécer Camargo M.
María Mercedes Corral S.

Editora Técnica
Denisse Cangrejo Aljure

Editora
Sara Gallardo Mendoza

Junta Directiva ACIS
2020-2022
Presidente
Luis Javier Parra Bernal
Vicepresidente
Sandra Lascarro Mercado
Secretario
Martha Juliana Ardila Arenas
Tesorero
Jaime García Cepeda
Vocales
Dalia Trujillo Penagos
Jorge Fernando Bejarano Lobo
Rodrigo Rebolledo Muñoz

Directora Ejecutiva
Beatriz E. Caicedo Rioja

Diseño y diagramación
Bruce Garavito

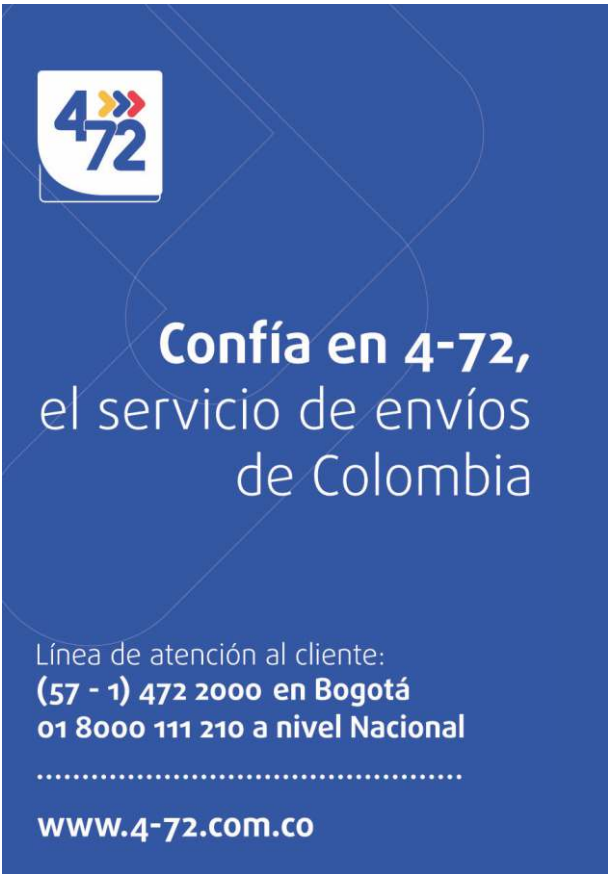
Los artículos que aparecen en esta edición no reflejan necesariamente el pensamiento de la Asociación. Se publican bajo la responsabilidad de los autores.

Julio - Septiembre 2020
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

NASCO
NACIONAL DE COMPUTADORES S.A.

APOYA ESTA PUBLICACIÓN

TEL: 6 06 06 06- CR 15 No 72-73




Habilite el rendimiento de red avanzada en la sucursal
Fortinet es el único proveedor de NGFW que proporciona Secure SD-WAN junto con protección avanzada contra amenazas, integrada desde la oficina central hasta la sucursal.
FORTINET
www.fortinet.com

Entornos IoT

DOI: 10.29236/sistemas.n156a1

¿La nube, la niebla o el borde?

Denisse Cangrejo Aljure

Sin duda, Internet de las Cosas −IoT− es un "término" relevante en la actualidad. A veces, usado para referir un concepto, o bien una tecnología, o un tipo de *hardware* que se suele llamar dispositivo o sensor, e incluso, el proceso de captura de datos con dichos sensores.

En efecto, Internet de las Cosas es todos ellos y posiblemente la mejor concepción para IoT es como un ecosistema tecnológico que involucra dispositivos, sensores, plataformas de procesamiento, infraestructura de redes, o bien, las aplicaciones de usuario final.

En dicho ecosistema surge un conjunto de tecnologías diversas, que habilitan IoT, dentro de las cuales la computación en la nube ha jugado

un papel preponderante. No obstante, la experiencia en cierta clase de aplicaciones IoT, ha mostrado la necesidad de plantear alternativas a la nube, que soporten la cantidad y variedad de datos sin precedente, generados por un número, creciente también, de sensores que hacen parte esencial del mundo de *Internet de las Cosas*.

Surge así en el año 2012, la *Computación en la Niebla*, o *Fog Computing*, concepto propuesto por CISCO e impulsado por el *OpenFog Consortium*, fundado tres años después, para promover su uso, diseminación y estandarización. Posteriormente, en 2019, este consorcio se fusiona con el *Consorcio de Internet Industrial de las Cosas*, confirmando con ello una evolución conjunta y complementaria, como parte de la transformación digital que vive la industria, en el siglo XXI.

Por su parte, *Edge Computing*, cuyo origen se remonta a los 90s[1], se ve luego impulsado por la *Computación Ubicua* al finalizar el pasado siglo. Para comienzo del nuevo siglo, el ecosistema está conformado por Internet de las Cosas que, según la aplicación y según las necesidades de escalabilidad y los requerimientos específicos de cómputo, puede involucrar en un sistema, perspectivas de arquitectura en la Nube y/o en la Niebla y/o en el Borde.

La Niebla y el Borde, conocidas como *Computación Perimetral*, particularmente ofrecen alternativas de solución a problemas que enfrentan los sistemas IoT, bajo la perspectiva centralizada de la Nube. Las más relevantes que, sin duda, se deben señalar con esta computación perimetral, son:

- Reducción de la latencia para diversas aplicaciones que requieren respuestas, incluso de milisegundos, como sistemas industriales, o financieros, en los cuales las decisiones son necesarias en tiempo real. Por eso se dice que estas alternativas "acercan" los datos al usuario final.

- Preservación de ancho de banda, porque la computación en el perímetro, evita el flujo de datos provenientes de cientos o miles de sensores a través de las redes, para ser llevados hasta los centros de datos de la Nube.

- Disponibilidad de los datos IoT cerca al usuario final, que en muchas situaciones supone una garantía de seguridad y de protección de su integridad.

- Aumenta la seguridad de la información, o dicho de mejor forma, reduce su vulnerabilidad, tanto en el tránsito desde los diferentes dispositivos que la generan, como en la nube, en donde son susceptibles a fallos o ataques que afectarían todo el sistema; la alternativa distribuida reduce po-

[1] Red de Entrega de Contenido (CDN), 1990 - Akamai.

tencialmente este riesgo a uno, o pocos nodos de la niebla o dispositivo en el borde.

- Acerca el procesamiento de los datos IoT, dando paso a su procesamiento en el lugar preciso, el borde o la niebla, si están asociados a decisiones muy sensibles, o bien la nube cuando se requiere procesamiento complejo como analíticas de *big data* o aprendizaje de máquina.

A la luz de estas consideraciones, resulta acertado dedicar este número de la revista a la *Computación en la Niebla y en el Borde,* tecnologías que ganan preponderancia e interés en la comunidad de ingenieros de sistemas, particularmente en el ámbito de Internet de las Cosas.

Es por esto que la *Asociación Colombiana de Ingenieros de Sistemas* −ACIS−, ha convocado a expertos de varios sectores y miradas diversas, quienes hicieron preciados aportes en la materia, que esperamos contribuyan al fortalecimiento de la comunidad a la que va dirigida la publicación.

Una primera perspectiva del tema, la presenta el exministro de Tecnologías de la Información y las Telecomunicaciones −TIC−, Diego Molano Vega, quien esboza el panorama global nacional, de cara a los desafíos de la transformación digital, y de una manera escueta deja al descubierto las dificultades y limitantes en infraestructura y en formación de expertos para comprender y adoptar dicha tecnología.

Incluye esta edición tres artículos, el primero de los cuales escribió Tatiana Delgado, vicepresidenta de la Unión de Informática de Cuba, tema que ofrece un acercamiento conceptual a *fog computing*, expone sus ventajas y los tipos de aplicaciones IoT para las cuales es más apropiado su uso, además de señalar los desafíos más importantes asociados a tal enfoque emergente.

Con un artículo sobre un tema de enorme sensibilidad y preocupación entre directivos y líderes de TI, como lo es la resiliencia organizacional, Jeimy J. Cano, director de esta revista, presenta los impactos y afectaciones de la transformación digital, a partir de tecnologías como *Fog y Edge Computing.*

Por su parte, el ingeniero Andrés Cantor conceptualiza sobre *Fog Computing* y se refiere a los pilares de una arquitectura del ámbito de IoT, que acerque la computación a los sensores y dispositivos. Con estas tres miradas se presenta al lector un panorama ilustrador que le permita acercarse a tecnologías perimetrales en sus proyectos de transformación digital.

Así mismo, el columnista invitado, Eduardo Alfonso Parra, desde el actual contexto de la pandemia, resalta las ventajas de la *Computa-*

ción en la Niebla y las soluciones que esta tecnología puede ofrecer en situaciones diversas de esta era digital.

La sección Cara y Sello presenta el resultado del foro académico realizado, el cual permitió en forma amena e interesante develar puntos de vista diversos sobre concepción y uso de la Computación en el Borde y en la Niebla, con tres participantes del sector empresarial de TI: los ingenieros Felipe Nicolás Diniello, desde Argentina, Juan Jurado desde Medellín, Colombia, y Julián Suárez desde España. Para los lectores de esta publicación, será un aporte valioso la mirada más globalizada de expertos de TI en el uso de estas tecnologías.

Para finalizar, la investigación realizada muestra una tendencia sobre conocimiento, conceptualización, comprensión y apropiación de estos nuevos campos de TI que se perfilan muy relevantes en el momento tecnológico actual.

Libia Denisse Cangrejo Aljure *Ingeniera de Sistemas, PhD en Ingeniería – Sistemas y Computación y Msc. en Geomática, de la Universidad Nacional de Colombia. Especialista en Teledetección, Cartografía y SIG de la Universidad Alcalá de Henares, España y especialista en SIG, de la Universidad Distrital Francisco José de Caldas. Desarrolló su tesis doctoral en el campo de Modelado Semántico de Contexto para el ámbito de Internet de las Cosas, con Linked Open Data. Docente de la Facultad de Ingeniería de la Universidad Nacional de Colombia. Ha participado y liderado proyectos de TI y Geoinformación en diversos campos, algunos de ellos de carácter social, como El SIG de Gestión Local para Ciudad Bolívar, en la Corporación SUR, Georreferenciación y Reingeniería para la Gestión del Conflicto Local de la Candelaria, Diseño conceptual del SIG para la Mesa Regional de Planeación Bogotá–C/marca, PNUDR/UNAL y el Convenio UNAL/MinTIC, Computadores para Educar, entre otros.*

Cloud, base fundamental para la recuperación económica

DOI: 10.29236/sistemas.n156a2

"La vida no es esperar que la tormenta pase. Es aprender a bailar bajo la lluvia"
César Évora

Eduardo Alfonso Parra G.

Casi cinco meses después de haber empezado una pandemia a nivel mundial debido al COVID-19, la mayoría de los empresarios del país y sus áreas de TI tuvieron que adaptar su cotidianidad para continuar con sus negocios, no solo por el teletrabajo, sino porque todos los procedimientos estaban pensados para hacerse de manera presencial y no virtual; lo importante para analizar no es cómo seguir sosteniendo a la compañía en la virtualidad, sino pensar qué se necesita cuando todo regrese a la "nueva normalidad".

Las cifras son contundentes, según un estudio de la *Federación Colombiana de Gestión Humana*[1], una de

cada dos empresas en Colombia no tenía a disposición políticas o esquemas para trabajo remoto previo a la pandemia. En un ejemplo sencillo muchas compañías entienden mal la digitalización de procedimientos y pretenden que sea digitalización; es el caso de la firma digital, que se puede hacer por una página o escanear, pero si este proceso no brinda una garantía legal o contractual, de nada sirve el medio.

La digitalización debe ser soportada en sistemas que garanticen confiabilidad y disponibilidad, con el fin de que en cualquier proceso contractual sean válidos legalmente; se trata de un asunto que necesita transformar la cultura organizacional e ir trasladándola a estados completamente digitales.

Según *Forbes*[2], cerca del 80% de los colombianos espera que las labores empresariales continúen siendo remotas, una vez se supere la emergencia sanitaria que ha generado el COVID-19, por lo que las compañías deben empezar a establecer las medidas tecnológicas para modificar esos cambios temporales y soportarlos en infraestructuras que garanticen una digitalización permanente en sus procesos.

Lo anterior, nos lleva a analizar cuál es la tecnología fundamental que nos ha permitido continuar con la productividad empresarial durante una emergencia como esta, encontrando que son los servicios en la nube (*Cloud Computing*) los que soportaron nuestros procesos, y es la tecnología que se requiere adaptar en la época post-Covid para aprovecharla en su máximo potencial.

Dentro de las características más importantes de la computación en la nube encontramos la flexibilidad, disponibilidad, rendimiento y escalabilidad, las cuales han facilitado migrar acciones que cotidianamente eran presenciales, a modelos virtuales con grandes beneficios, como poder tener reuniones con empleados, proveedores y clientes, a través de servicios de videoconferencia; gestionar de manera remota el flujo de información, cumpliendo los protocolos de seguridad sin importar la ubicación de los empleados o haber podido mantener a las empresas al día en sus obligaciones financieras y en el recaudo de sus ingresos, con el uso de los sistemas de pago electrónicos, para mencionar solo algunas de las actividades laborales que hemos modificado en estos meses.

Estas funcionalidades se han soportado en el esquema de servicio más usado entre las opciones que ofrece la computación en la nube, catalogada como SaaS (*Software como Servicio*), que permite a las

[1] https://www.dinero.com/empresas/articulo/empresas-de-colombia-no-estaban-preparadas-para-el-teletrabajo/289260. Recuperado julio de 2020.

[2] https://forbes.co/2020/06/09/capital-humano/80-de-los-colombianos-quiere-seguir-teletrabajando-despues-del-aislamiento/. Recuperado julio de 2020.

compañías no preocuparse por equipamiento o configuraciones, sino solicitar el tipo de *software* que se requiere, dando lugar a que esta simplicidad atraiga a los empresarios y sea el modelo más usado, que según Gartner[3] crecerá a una tasa del 15,5% en los próximos cinco años.

Sin embargo, el modelo SaaS no cubre algunas de las características importantes en el momento de llevar los modelos laborales a esquemas de trabajo remoto permanente, para facilitar a las empresas tener infraestructuras variables, en las que el procesamiento, el almacenamiento y los puestos de trabajo puedan ser virtuales, con despliegues mucho más ágiles y con costos por uso, trayendo un concepto de elasticidad que brindará a las compañías eficiencias en costos operativos y de calidad de servicio al cliente, lo cual se logra con el modelo de Infraestructura como servicio (IaaS), que es el segundo más usado en los modelos ofrecidos en *Cloud Computing*.

Analizando las ventajas que puede traer la implementación de servicios en la nube por parte de empresas en Colombia, se puede aprender de los problemas presentados durante los días sin IVA en Colombia[4], que generaron quejas de usuarios por tener que esperar en filas digitales por mucho tiempo, sumado a los problemas en el despacho de artículos en los tiempos ofrecidos, por la falta de una sincronización entre los inventarios de las ventas físicas y las ventas virtuales y los múltiples engaños que se generaron en redes usando este día como mecanismo para estafar a usuarios inexpertos. Pues bien, es aquí donde entra en contexto todo lo que se ha documentado en este escrito y donde vienen los retos de la vida pos-COVID-19.

Todos estos problemas se pueden superar con la implementación de herramientas tecnológicas ofrecidas por la computación en la nube para automatizar procesos y responder ante requerimientos de clientes en un tiempo mucho menor. Para entender cómo sería, lo trasladamos a un ejemplo más claro; tomaremos el problema de las filas virtuales, el cual se presentó debido a que la capacidad de respuesta de los servicios en la *web* fueron superados ampliamente y al tener servidores físicos no disponían de la capacidad para crecer en función de la demanda del momento.

Si estas empresas tuvieran implementados servicios en la nube, la ampliación de la infraestructura necesaria para cumplir con la demanda, se puede hacer en menos de un minuto y genera costos únicamente por las horas que estén activas; así,

[3] https://hbr.org/2020/07/a-guide-to-building-a-more-resilient-business?ab=hero-main-text

[4] https://www.eltiempo.com/economia/sectores/dia-sin-iva-esto-fue-lo-que-gastaron-los-colombianos-en-esta-segunda-jornada-514162. Recuperado julio de 2020.

la respuesta a los usuarios no debería haber sido a través de filas virtuales, sino mejorando su capacidad de respuesta en la nube, con un impacto económico mucho menor y con un impacto reputacional muy beneficioso.

La computación en la nube proporciona elasticidad tecnológica a las empresas para crecer o reducirse según las necesidades, de manera que esa capacidad impacte la economía de la organización solamente por lo que en efecto está usando y no por la adquisición de equipos o *software* que no se use o se subutilice

Cuando los tiempos de entrega de las compras no se cumplen o cuando el producto adquirido no pudo ser entregado, es allí donde podemos ver la problemática de tener procesos por silos, no encadenados, en procesos digitalizados y automatizados como demanda la prestación de servicios en la era de la transformación digital, a la que todas las empresas se han visto obligadas a acelerar su implementación por esta coyuntura.

Estos problemas se pueden solucionar con sistemas digitalizados de inventarios, que apoyados en Internet de las Cosas (IoT), mantienen completamente actualizada la capacidad real de servicios o productos, además de permitir una trazabilidad en la entrega, proporcionando al cliente final una experiencia satisfactoria en cuanto a los tiempos, como en el seguimiento de los productos adquiridos, sin importar si fueron compras presenciales o virtuales.

Uno de los mayores obstáculos que siempre ha tenido y tiene la implementación de los servicios en la nube por parte de las empresas, es la discusión sobre si es seguro, si se pierde el gobierno y la privacidad de la información. Lo cual sin duda es un temor válido por parte de los empresarios, pero que con los avances se ha podido minimizar cada día, teniendo siempre claro que la seguridad al 100% no existe, ni en el entorno físico ni en el virtual. La seguridad, es un riesgo que se debe gestionar y tener en cuenta desde la planeación y la migración, pero jamás se debe temer o ver como un obstáculo, para no dar ese paso necesario en nuestros días.

Al tener claro que la seguridad de la información es esencial en la transformación digital y en las implementaciones de los servicios en la nube, las compañías pueden establecer con sus proveedores de servicios de nube, las herramientas y monitoreos necesarios y suficientes para garantizar un control que reduzca la probabilidad de ser víctimas de un ataque cibernético, con costos reputacionales y económicos de gran impacto para las empresas.

Pero el gramo de oro sobre el que vienen las apuestas de la nueva normalidad y que seguramente

brindará grandes soluciones para las organizaciones y sus empleados en el mundo post-COVID, es la solución de escritorios virtuales (VDI), la cual permite tener de forma inmediata la cantidad de equipos de cómputo que realmente se requieren, reduciendo o aumentando según sus necesidades, a través de servicios de virtualización para facilitar las operaciones del área de sistemas, en cuanto a mantenimiento, la instalación de *software*, copias de seguridad, etc.

Además, facilita el despliegue del trabajo remoto, toda vez que el empleado puede acceder a su equipo corporativo desde cualquier equipo, en cualquier lugar del mundo, manteniendo control de la información y mejorando la seguridad de la misma, pues toda la información que generen los empleados ya no reposa físicamente en el equipo donde se realizó, sino que se encuentra en el servidor central de virtualización, dejando así la necesidad al empleado de tener cualquier tipo de equipo de trabajo y sólo mediante una conexión a internet para llevar a cabo sus tareas de trabajo.

Como se pueden dar cuenta, las ventajas en el entorno *Cloud*[5] saltan a la vista y están a disposición de todos para ser usadas. Además, es innegable el aporte que ha tenido esta tecnología en la resolución de problemas a los que nos hemos visto obligados a responder; pero sin duda, serán más las demandas que necesitarán las organizaciones en un mundo que, sin lugar a dudas, cambió y que nos obliga a enfrentarnos a una nueva realidad y por ende, a nuevos retos.

El *Cloud* no solo facilita la resiliencia en las organizaciones, también se ha convertido en un instrumento y en un medio para hacer el mundo más humano en esta coyuntura; es por eso que invito a todos los empresarios, en especial a los de las pequeñas y medianas compañías, a involucrarse en esta aventura que los llevará a hacer cosas distintas, más enfocadas en sus clientes, óptimas para sus procesos y que los hará mucho más relevantes en el mercado.

[5] https://www.muycomputerpro.com/2020/07/16/las-empresas-espanolas-teletrabajan-en-la-nube. Recuperado julio de 2020.

Eduardo Alfonso Parra González. *Cuenta con doce años de experiencia liderando temas digitales y modelos de transformación digital para las empresas, diseño de nuevos modelos o sistemas de comunicaciones de Seguridad de la Información, Cloud y Continuidad del Negocio. Es Ingeniero en telecomunicaciones de la Universidad Santo Tomás de Bogotá y Especialista en seguridad de la información de la Universidad de Los Andes. Actualmente, se encuentra realizando estudios en PRIME (Universidad Sergio Arboleda) de un EMBA. Además, es certificado en ISO27000, COBIT, CBCP (Administración de Continuidad de Negocios) y CISM (Certified Information Security Manager). Se ha desempeñado como Oficial de seguridad de la información en la Compañía de Profesionales de la Bolsa, como Consultor Senior en KPMG y como profesor de cátedra en el Politécnico Gran Colombiano y en la Universidad Santo Tomás. Desde el 2013 se encuentra vinculado a Telefónica Movistar Colombia y desde el 2017 se desempeña como Gerente de Seguridad y Cloud en la misma Organización.*

NEOSECURE
SABEMOS DE SEGURIDAD

EXPERTOS EN CIBERSEGURIDAD

Somos una compañía de Ciberseguridad con más de 20 años de experiencia dedicada a enfrentar las amenazas, proteger los activos y sistemas de las organizaciones. Nos actualizamos constantemente en tecnologías y procesos para estar a la altura de las nuevas amenazas, basados en la INNOVACIÓN y el SABER DE SEGURIDAD. Siempre a la vanguardia en Latinoamérica en el desarrollo de la Ciberseguridad.

Seguridad Corporativa	SGS	Identidad Digital	Seguridad OT	Consultoría

Avenida Calle 26 No 69 D 91 Of 504 Torre El Dorado. Bogotá D. C. - +57 1 432 0700
info@neosecure.com
Visítanos en www.neosecure.com

Diego Molano Vega: ¿Colombia en retroceso?

DOI: 10.29236/sistemas.n156a3

Maneja el mapa completo del país, lo observa, sugiere y recomienda. Describe las carencias y plantea soluciones.

Sara Gallardo M.

Diego Molano Vega, exministro de Tecnologías de la Información y las Telecomunicaciones (TIC), consultor internacional de gobiernos y empresas en transformación digital ubicado en Washington, presidente de la universidad Área Andina, asesor senior del Banco Interamericano de Desarrollo (BID), de Mckinsey y de la OECD, entre tantas otras responsabilidades, tiene el país completo en su ejercicio profesional.

No lo desvelan esas múltiples ocupaciones ni el otro montón como investigador de varios centros de pensamiento en los Estados Unidos. Le quita el sueño la educación de sus hijas de dos y cuatro años en estos tiempos de pandemia.

“Ellas son muy chiquitas y a los 10 minutos están fatigadas con cualquier actividad inspirada en tecnología. Las escuelas están cerradas posiblemente hasta febrero y no

podemos parar su educación seis o siete meses, así que el reto es inmenso", por esa razón uno de sus proyectos inmediatos apunta a la creación de una escuela para formación de padres.

Reconocido en el mundo como una de las 100 personas más influyentes en asuntos de gobierno digital y el número 20 en ambientes Fintech de Iberoamérica, atendió esta entrevista con la sencillez del boyacense y la firmeza de un profesional muy experimentado y conocedor del sector como ninguno.

Razones suficientes para dejarlo hablar sobre Colombia desde todas sus aristas, enfatizar en las carencias y destacar las fortalezas. Sin abordar puntualmente las inquietudes preparadas para la entrevista, alrededor de la computación en la nube y en la niebla, sus respuestas muestran el estado del país, más allá de estos nuevos desarrollos tecnológicos.

Revista Sistemas: *¿Cómo define usted la tecnología de la computación en el borde y en la niebla en Colombia?*
Diego Molano Vega: Es un paso más en los avances tecnológicos y suministra nuevas oportunidades a un país como Colombia y facilita el acceso a los últimos desarrollos, más rápido y en forma más modular.

RS: *¿Cuál es el estado de Colombia en términos de infraestructura tecnológica?*

DMV: La mejor analogía para responder a su pregunta es la bicicleta, quien no pedalea, se cae. En otras palabras, es necesaria una permanente inversión para renovarla y esa debería ser la tendencia, tal y como sucede con los teléfonos celulares; por lo general, las personas cambian de equipo cada dos años, así que las empresas y el Gobierno no pueden dejar de invertir recursos y esfuerzos en ese cambio.

Por fortuna, las tecnologías disponibles en la nube permiten el acceso de los usuarios a lo más reciente, de acuerdo con las necesidades individuales.

RS: *Es inevitable no referirse a la pandemia y la situación del país, ¿Colombia está en condiciones de hacer las inversiones necesarias en aras de fortalecer la infraestructura, para como dice usted pedalear y no caernos?*

DMV: Hay que ver para qué y en dónde. Considerando las brechas que tiene Colombia, éstas son de muchos tipos. La primera relacionada con la infraestructura, medida a través de un índice del Foro Económico Mundial y del Portulans Institute −soy miembro de la Junta Directiva−, que ubican a nuestro país en el puesto 67 en términos de infraestructura tecnológica, por encima del promedio en América Latina; y establece en 70% los colombianos conectados a Internet. Con base en tales cifras y en lenguaje coloquial, el vaso se puede ver medio vacío o medio lleno. Yo lo veía medio lleno en mi gestión ministerial, lo que no quiere decir que se frene la inversión en fibra óptica para los hogares y, sobre todo, para los de estratos bajos.

RS: *Ese 30% que no está conectado a Internet pertenece a los estratos más bajos del país, grupo de población desprotegida y con grandes carencias, particularmente en esta pandemia. ¿De acuerdo?*

DMV: Exactamente. Colombia está muy bien conectada internacionalmente, tiene 14 o 15 cables submarinos en el Pacífico y el Caribe y muy bien interconectada dentro del país. Nosotros pusimos fibra óptica y llegamos al 96% de los municipios, también trabajamos en redes de alta velocidad para llegar al resto de cabeceras municipales. En las autopistas que unen las ciudades estamos muy bien, nos falta mejorar en las callecitas de tales autopistas de la información, con el propósito de llegar a cada negocio, cada escuela y cada hospital. En otras palabras, trabajar sobre lo que llamamos el último kilómetro, en el que se requiere una fuerte inversión, para el despliegue de las redes 5G.

RS: *Y ¿la pandemia ha frenado ese recorrido? ¿Nos quedamos estáticos?*

DMV: Las inversiones han continuado, a pesar de que hace un par de años tuvieron una frenada muy dura, ocasionada básicamente por el pago impuesto a las firmas Claro

y Telefónica, por un Tribunal de Arbitramento. Si estas compañías tienen que pagar casi cinco billones de pesos, dinero que no se fue para el sector, sino para tapar el hueco fiscal, recursos que se dejaron de invertir en infraestructura para el sector de las telecomunicaciones, lo que generó una sensación de debilidad en el marco regulatorio. Han pasado varios años y se ha empezado a recuperar credibilidad, después de un buen tiempo en que no había confianza para invertir en el país. La acción en contra de esas dos compañías, sumada a la carga tributaria del sector, tan excesivamente alta −la telefonía celular paga cerca del 23% de IVA−, son medidas absurdas. Además, con una reforma tributaria anual, con unas reglas de juego sujetas a cambio con tanta frecuencia es difícil atraer inversión.

RS: *En ese contexto que usted describe ¿significa que vamos pedaleando, pero en reversa?*

DMV: Seguimos pedaleando, pero muchos países van más adelante que nosotros. Por ejemplo, México, Costa Rica y Uruguay que van avanzando rápido. México ahora tiene una muy buena oportunidad por la entrada en vigor del nuevo tratado de libre comercio con Estados Unidos y Canadá, país que tiene novedades en materia de Comercio Digital. Por otro lado, hay que considerar que en términos de infraestructura, no se contempla solamente lo que está en las calles, sino la que está dentro de las casas de los consumidores. La pandemia ha puesto al descubierto que en los hogares colombianos faltan buenas redes en el interior, además de una buena conexión *wifi*; y, sobre todo, computadores. ¿Cuántos hogares están habilitados para asumir la educación de los hijos en esas condiciones, particularmente cuando tienen tres estudiantes y un único equipo? Una casa típica colombiana está conformada por papá, mamá y dos o tres hijos. Las estadísticas muestran que todos están conectados a Internet, pero con un solo computador y eso no es suficiente.

RS: *Y ¿qué solución ve usted en el corto plazo? ¿Alguna propuesta?*

DMV: Hay que realizar acciones para reducir los impuestos en todo tipo de terminales de computación, tanto aranceles como IVA; bajar los precios de todos los equipos, como lo hicimos en su momento en la administración Santos, pero que al final de la misma se fue perdiendo por las reformas tributarias que iban eliminando esas ventajas. Así mismo, eliminar el IVA para todos los servicios de telecomunicaciones, esta es una forma de multiplicar la economía; cuando todos estamos en el mundo digital y el sector tiene ese tipo de cargas, la situación es muy difícil. Una pequeña ventaja hoy es que los servicios en la nube están exentos de IVA, pero las conversaciones apuntan a que en la próxima reforma tributaria se volverá a aplicar, hecho que sería gravísimo.

***RS:** ¿Retomamos la descripción de las brechas?*
DMV: La segunda brecha tiene que ver con que la gente está conectada, pero no, en la manera como usa la tecnología. Colombia comparada con países como Corea o algunos del norte de Europa, refleja un atraso en aumento. Aunque en la pandemia la situación ha mejorado, en Bogotá pasamos del 4% de los teletrabajadores, al 25%. De acuerdo con estudios del Centro Nacional de Consultoría, antes de la pandemia el 85% de los colombianos utilizaba Internet solo como una herramienta de comunicación básica o de entretenimiento, ahora lo hace en una forma más productiva.

La siguiente brecha tiene que ver con la forma en que el Gobierno usa la tecnología y ahí sí que el retraso es considerable. De liderar en 2014 los *rankings* de América Latina y de estar inclusive entre los países con mayor participación de la ciudadanía en el uso de servicios por medios electrónicos, el panorama hoy es muy distinto, vamos en descenso; de ocupar el puesto número 50 hoy estamos en la posición 67.

***RS:** ¿A qué se debe?*
DMV: A que el pedaleo al que me he referido debe ser permanente y en una forma innovadora, no siempre hay que hacer lo mismo. En el mundo digital vemos una tendencia muy válida en el ambiente de *Start-ups* y encontramos muchas firmas colombianas; los emprendedores prestan servicios a las entidades del Estado y es necesario contemplar la forma de ayudarlas para dar paso al ofrecimiento de varios servicios como sistemas de *data analytics* para el Estado, seguridad y ciberseguridad entre otros. En esa dirección no vamos al mismo ritmo del mundo, no significa que estemos detenidos, pero no vamos tan rápido como deberíamos.

***RS:** En su opinión ¿cómo está la empresa privada?*
DMV: Las empresas privadas no se están transformando digitalmente a la velocidad que deberían hacerlo, como lo están haciendo, por ejemplo, Asia y el norte de Europa. Hay algunos sectores en que vamos bien, como el financiero.

***RS:** Supongo que se refiere a las pequeñas y medianas empresas, ¿verdad?*
DMV: Sí y considerando que en ese sector está la gran mayoría de empleos, la situación es preocupante. Si no hay transformación digital desaparecerán con rapidez y serán reemplazados por modelos de negocios extranjeros. En el mundo digital no existen fronteras y ante esa carencia, los nuevos empleos serán cubiertos desde afuera del país. Hecho directamente relacionado con la brecha más grande que tenemos alrededor de las necesidades de talento digital, por encima de la infraestructura, del uso del Gobierno de los medios digitales para ofrecer servicios o si las

empresas se están o no transformando. Específicamente, la necesidad apunta a cuatro tipos de talento. El primero compuesto por programadores y está representada en más de 100.000 en el corto plazo.

RS: *Pero ¿cómo, si los estudiantes de ingeniería de sistemas ya no quieren ser programadores?*
DMV: Esa situación es muy preocupante. El segundo talento se basa en la necesidad de que todos los profesionales tengan un poquito de ingenieros de sistemas. A los comunicadores, por ejemplo, se les pregunta ¿cómo funciona el algoritmo de la publicidad de *Google*?, y no tienen ni idea. En otras palabras, estamos formando profesionales para el siglo pasado. Hay que formar ingenieros de sistemas, pero insisto en las habilidades que exige este nuevo mundo. En la universidad Área Andina, de la cual soy presidente, lo denominamos 'humanismo digital'. El tercer talento está representado en las mujeres −a propósito, me alegra muchísimo que la Junta Directiva de Acis esté conformada por mujeres−. Es inminente que masivamente ellas salgan a trabajar; no se trata de un asunto de igualdad de género, es que necesitamos una economía más productiva y las mujeres cuentan con mayores habilidades para esa transformación, que los hombres.

RS: *¿Por qué?*
DMV: Tienen más habilidades blandas que los hombres; es decir, de empatía, de comunicación, que en nuestra cultura los hombres no las hemos desarrollado.

Y el cuarto talento se basa en la formación de líderes para esta revolución. Y no los tenemos. Busquemos cinco candidatos para ser ministros en la transformación digital desde sus respectivos sectores y no se encuentran.

RS: *¿Y cuál es la solución? Pareciera que estamos en un círculo vicioso y sin salida.*
DMV: La solución está en que cada uno de nosotros nos apersonemos del asunto; no se trata de que 'papá' Gobierno venga a hacerlo. Las oportunidades son visibles para programadores y líderes, están a la mano. Y quien adquiera esas habilidades encontrará sin dificultad oportunidades laborales y sus negocios serán más exitosos.

RS: *Hablemos ahora sobre el marco regulatorio que soporta la tecnología en Colombia. ¿Qué opina al respecto?*
DMV: Antes era un marco regulatorio de telecomunicaciones muy específico, hoy en día es transversal y contempla diferentes sectores como el financiero, el e-commerce, la salud para regular la historia clínica electrónica, la justicia para promover el expediente judicial electrónico, otro laboral que promueve el teletrabajo. Ahora el de las telecomunicaciones es el menos relevante y se trata de una la-

bor conjunta, no de un único ministerio.

RS: *Poco hablamos de los asuntos inherentes al tema central de la revista: la computación en el borde y en la niebla, pero teniendo en cuenta su condición de exministro de las TIC, son importantes otros temas. Por ejemplo, la seguridad y la ciberseguridad. En su opinión ¿cómo está el país al respecto?*

DMV: Ahí también carecemos de talento. Necesitamos más profesionales que manejen estos asuntos, pero también que los ciudadanos seamos conscientes de los riesgos relacionados con la ciberseguridad. Y hay que avanzar en dos frentes alrededor de la capacitación. Por un lado, disponer de profesionales que ayuden al Gobierno y al sector privado para evitar eventos y proteger los sistemas de información. Pero, también informar a los ciudadanos y capacitarlos sobre las buenas prácticas en búsqueda de la seguridad.

RS: *Ahora sí sobre el tema central de esta edición. ¿Colombia puede aprovechar el ambiente de la computación en el borde y en la niebla?, ¿es posible habilitar esa promesa de valor de la cuarta revolución industrial?*

DMV: Claro que sí, pero con gente capacitada.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; es editora de esta revista.*

GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Somos el primer proveedor MSSP* Fortinet en Colombia

*Managed Security Service Provider (Proveedores de servicios de seguridad administrados)

FORTINET

Generando confianza y mejorando la ***experiencia*** de nuestros clientes

FIRST Improving Security Together

CERT

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

International Organization for Standardization ISO 27001

Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147
Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Santander | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

@GammaIngenieros Gamma Ingenieros Gamma Ingenieros

www.gammaingenieros.com

Computación en el borde y en la niebla

DOI: 10.29236/sistemas.n156a4

Tendencias e inmersión

Resumen
La *Computación en el borde y en la niebla* contempla estrategias para extender el paradigma de *Computación en la nube*, adoptado en forma amplia hoy por hoy, en el ámbito organizacional e incluso personal. Ha adquirido importancia creciente en los últimos años como una alternativa en modelos centralizados, que ofrece respuestas a retos latentes en las aplicaciones del entorno de Internet de las Cosas.

A la luz de este panorama tecnológico, la *Asociación Colombiana de Ingenieros de Sistemas (Acis),* realizó una encuesta en el contexto nacional, dirigida a ingenieros de sistemas y computación, con el fin de conocer su opinión, conocimiento y grado de aplicación de estas dos tecnologías, "*computación en el borde*" y "*computación en la niebla*", cuyos resultados y reflexiones, son presentadas en este artículo.

Palabras clave: Computación en el Borde (*Edge Computing*), Computación en la Niebla (*Fog Computing*), Internet de las Cosas (IoT), Seguridad.

Introducción

El escenario tecnológico definido por Internet de las Cosas y por aplicaciones que demandan respuesta en tiempo real, plantea al sector empresarial y a los desarrolladores en el campo de la tecnología de información y las comunicaciones, desafíos de carácter funcional y tecnológico. La *Computación en la niebla* y la *Computación en el borde* constituyen una alternativa para hacer frente a algunos de esos desafíos como la movilidad, la respuesta en tiempo real y el uso eficiente de recursos.

La primera ofrece un mejor procesamiento de los datos para las aplicaciones basadas en la nube, el cual realiza más cerca de la fuente de los mismos, en el borde de la red. Gracias a esta característica se alcanzan beneficios como: menor latencia entre la aplicación cliente y el servicio en la nube; acercamiento del usuario y dispositivos a los contenidos con un uso más eficiente de los recursos de red y habilitación de la infraestructura de red futura.

Por su parte, la *Computación en la Niebla* enfatiza en el procesamiento en la infraestructura local de red, más que en los dispositivos y extiende los recursos de computación hacia el borde de la red, en un modelo distribuido. Así, se dispone en el borde de los servicios de procesamiento, almacenamiento y monitoreo provistos por el enfoque tradicional en la nube, por medio de instancias denominadas "*fog nodes*", las cuales realizan un procesamiento previo de los datos a la nube, en los dispositivos IoT ubicados en el borde, con beneficios potenciales como: menor latencia entre los dispositivos de usuario final y los nodos en la niebla; soporte a requerimientos de movilidad; habilitación de la ubicuidad de los servicios de computación y viabilidad de interacciones en tiempo real.

No obstante, la computación en la niebla y en el borde, tiene retos vislumbrados en el escenario tecnológico actual, asociados con los costos adicionales de *hardware* para el procesamiento local, las fallas de seguridad y confiabilidad de los dispositivos o de la red, o bien, el mantenimiento y control, retos que la computación centralizada en la nube no incluye.

A la luz de este panorama tecnológico, Acis realizó la encuesta *Computación en el borde y en la niebla, tendencias e inmersión,* dirigida a ingenieros de sistemas y computación, cuyos resultados reflejan la opinión, conocimiento y grado de aplicación de estas dos tecnologías, analizados en este documento.

La encuesta fue realizada durante los meses de julio y agosto de 2020, incluyó 10 preguntas orienta-

das a detectar el grado de conocimiento y apropiación de *Fog y Edge Computing* por parte de los ingenieros las organizaciones en donde se desarrollan profesionalmente. Los resultados muestran un universo de *86 encuestas* diligenciadas al *100%* y un tiempo de respuesta promedio de seis minutos y ocho segundos. Para la aplicación de esta encuesta se utilizó la herramienta abierta *SurveyMonkey.*

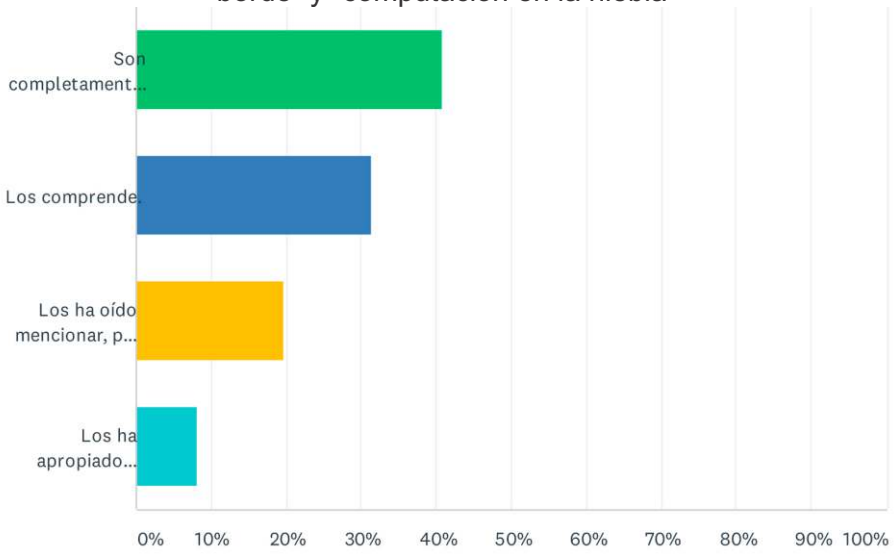
Resultados de la encuesta

En este aparte se presentan los resultados de las 10 preguntas que componen la encuesta con el correspondiente análisis individual y global, en los cuales se evidencia no solo el grado de apropiación, sino el impacto actual y potencial asociado a las tecnologías *Fog y Edge computing* y que puede servir de base para fomentar su difusión y uso en proyectos de ingeniería y desarrollo asociados con TICs y particularmente en el entorno demarcado por Internet de las Cosas, que sin duda permea espacios laborales y personales de la vida, en el siglo XXI.

Pregunta 1: Conocimiento y comprensión de *Fog* y *Edge Computing*

Es fundamental estimar el grado de conocimiento de estos dos conceptos y las tecnologías asociadas en

Figura 1. En su práctica profesional, los conceptos: “computación en el borde” y “computación en la niebla”



OPCIONES DE RESPUESTA	RESPUESTAS	
Son completamente nuevos.	40.70%	35
Los comprende.	31.40%	27
Los ha oído mencionar, pero no los comprende.	19.77%	17
Los ha apropiado (usted o su empresa), o ha utilizado tecnologías que sebasen en ellos.	8.14%	7
TOTAL		86

la práctica profesional de ingenieros y desarrolladores e identificar en qué medida se están aplicando.

En la Figura 1, los resultados revelan un panorama incipiente de conocimiento, en un 60.47% de los encuestados, para quienes son conceptos totalmente nuevos o que han oído mencionar, pero no comprenden. No obstante, un 31.4% de los encuestados manifiesta comprenderlos, porcentaje relevante, que da cuenta de una dinámica en curso, que potencia un índice de aplicación en un futuro próximo y deja entrever un posible nicho para el fomento de iniciativas que apliquen *Fog y Edge computing.*

Sin embargo, es necesario reconocer según estos resultados, que estos conceptos son nuevos para la mayoría de los encuestados, y la apropiación de estas tecnologías puede ser baja en el momento actual del país.

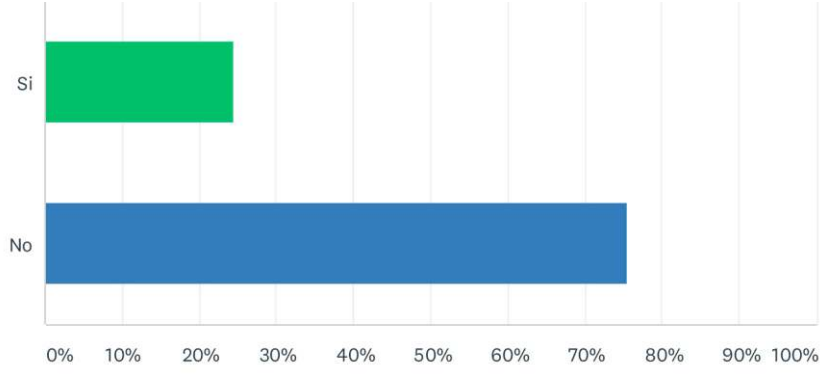
Pregunta 2: Uso de servicios de cómputo *Fog / Edge Computing*

En ecosistemas como el definido por Internet de las Cosas, caracterizados por el tiempo real, la necesidad de una baja latencia, aplicaciones distribuidas geográficamente y dispositivos capaces de procesar *in situ*, resulta más que ideal acercar los servicios al usuario de aplicaciones.

Tales opciones contemplan servicios de almacenamiento, infraestructura, y procesamiento de los datos, sin necesidad de ir hasta la nube, la cual aparece “lejana” para muchas aplicaciones IoT.

Por otra parte, en los modelos actuales de negocio, el acceso a ser-

Figura 2. ¿Conoce y/o ha utilizado algún servicio de cómputo en el borde (*edge computing*) o en la niebla (*fog computing*)?



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	24.42%	21
No	75.58%	65
TOTAL		86

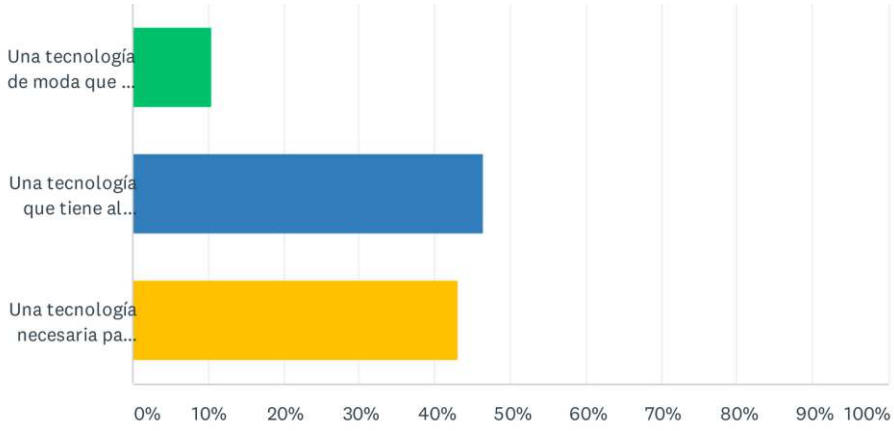
vicios es una alternativa muy atractiva que permite a las empresas crecer con sistemas escalables, cuyo costo de actualización, infraestructura, costos de actualización e incluso formación de expertos en TI, se traslada a los proveedores de servicio, dando paso con esto, incluso a una mejor planeación y gestión de gastos.

A pesar de esta tendencia global hacia el uso de servicios y de las ventajas que ofrecen la computación en la niebla y en el borde especialmente en aplicaciones de internet de las cosas, los resultados obtenidos en la encuesta sobre este particular, señalan una proporción de 3 a 1 (Ver Figura 2), en la cantidad de personas o empresas que no conocen ni han usado algún servicio de cómputo *fog / edge* y quienes sí los conocen. Esto de manera decidida, sugiere la necesidad de adelantar más iniciativas de difusión sobre estas tendencias y alternativas tecnológicas, como la que persigue Acis en esta edición de la revista *Sistemas* y con la encuesta misma, objeto de análisis. El mayor conocimiento de estos conceptos, de sus tecnologías asociadas y análisis de casos de uso, serán esenciales, para la adopción de este tipo de servicios y modelos de arquitecturas.

Pregunta 3: Necesidad de la computación en el borde o en la niebla.

La confianza de las empresas y profesionales de TI juega un rol fundamental en el proceso de evolución de tecnologías como estas, objeto de la encuesta realizada, proceso que será exitoso, en la medida en que efectivamente se apro-

Figura 3. En su opinión la computación en el borde o en la niebla es:



OPCIONES DE RESPUESTA	RESPUESTAS	
Una tecnología de moda que no llegará a masificarse.	10.47%	9
Una tecnología que tiene algún potencial competitivo para su empresa.	46.51%	40
Una tecnología necesaria para garantizar una ventaja competitiva en su empresa.	43.02%	37
TOTAL		86

pien y apliquen; en ese orden de ideas, los resultados obtenidos para esta pregunta son bastante alentadores, de cara a las posibilidades que tienen estas tecnologías. La Figura 3 muestra un escenario en el cual sólo un 10% no espera el uso masivo de estas tecnologías mientras que la gran mayoría (un 89.52%), percibe en ellas potencialidad en relación con la ventaja competitiva para sus empresas y casi la mitad de ellos, le otorga un carácter esencial para alcanzar tal ventaja competitiva.

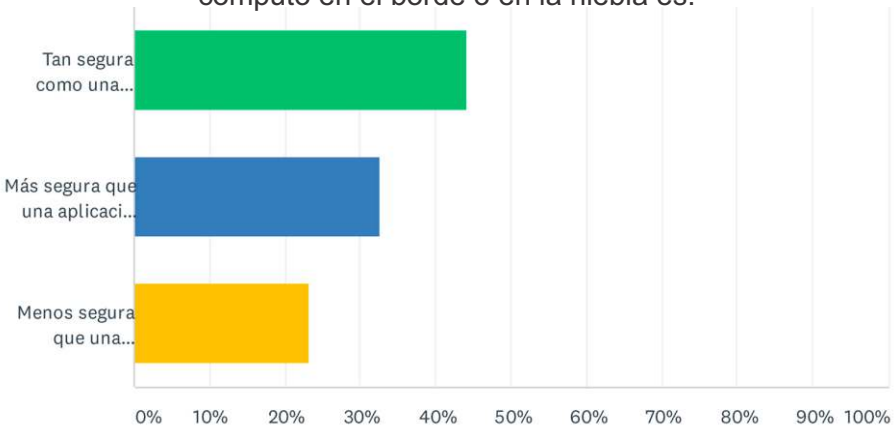
La competitividad, junto con los costos, el acceso distribuido, la escalabilidad y disponibilidad, entre otros, son factores a tener en cuenta en la elección de una alternativa tecnológica, en el momento actual y estos factores obtienen una buena valoración en el caso de la *Computación en el borde y en la niebla*. Es posible que las respuestas obtenidas obedezcan a este tipo de análisis, lo que justifica ese 89.52% de respuestas que asocian competitividad con estas tecnologías.

Pregunta 4. Seguridad en el borde y en la niebla *vs* la nube

En un escenario que alienta la generación continua de datos en forma masiva, el almacenamiento y procesamiento en servidores externos, algunas veces públicos y la transferencia de datos empresariales y personales fluyendo por redes externas, la seguridad y privacidad de los datos, en muchos casos sensibles, debe ser un criterio a considerar.

Si bien la primera disyuntiva de cara a la seguridad es elegir un proveedor de servicios como infraes-

Figura 4. Considera que una aplicación que utiliza un componente de cómputo en el borde o en la niebla es:



OPCIONES DE RESPUESTA	RESPUESTAS	
Tan segura como una aplicación con servicios en la nube.	44.19%	38
Más segura que una aplicación que usa los servicios en la nube directamente.	32.56%	28
Menos segura que una aplicación que usa directamente los servicios en la nube.	23.26%	20
TOTAL		86

tructura, plataforma o *software* interno o externo, esta pregunta de la encuesta abordaba una disyuntiva más: si al ser externo, se percibe mayor seguridad en la nube, o en la niebla o el borde. La seguridad y también la privacidad de la información es un asunto de interés ante la adopción de nuevas tecnologías, es una constante.

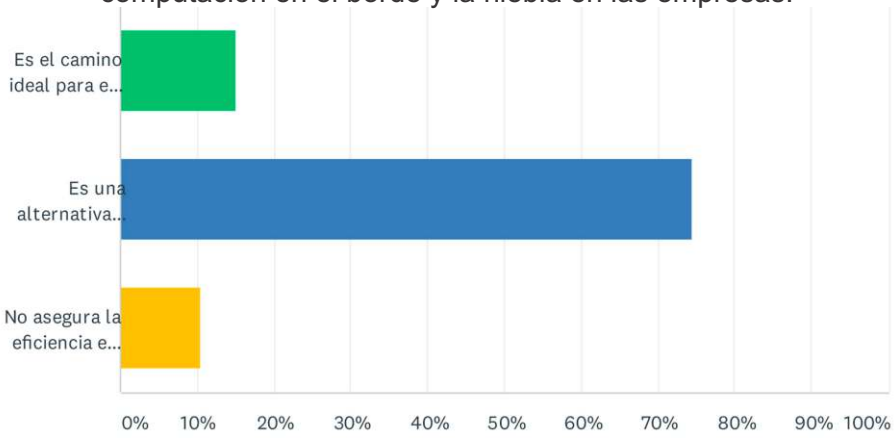
Sin embargo, los resultados de la encuesta parecen reflejar una baja preocupación; la mayoría, más del 76%, considera que la computación en el borde es tanto o más segura que la computación en la nube y probablemente este resultado evidencia desconocimiento de los riesgos por parte del público general, más que confianza objetiva en la tecnología. (Ver Figura 4).

Pregunta 5: Eficiencia en el procesamiento de los datos en el borde o en la niebla

Para dar respuesta a los retos de velocidad, variedad y volumen de los datos IoT, Cisco[1] plantea requerimientos asociados a la latencia, el ancho de banda de la red, la seguridad, la integridad y disponibilidad de la infraestructura y los datos, la gestión de datos distribuidos geográficamente y ubicar los datos en el mejor lugar para su procesamiento. Tales requerimientos no son satisfechos completamente en las arquitecturas tradicionales de computación en nube. Propone, por tanto, procesar la mayoría de

[1] CISCO, 2015 - *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are*

Figura 5. En un escenario IoT de "cosas" autónomas que capturan información, las soluciones tecnológicas deben privilegiar el procesamiento eficiente y en tiempo real de los datos. Considera usted que la adopción de la computación en el borde y la niebla en las empresas:



OPCIONES DE RESPUESTA	RESPUESTAS	
Es el camino ideal para el procesamiento eficiente de los datos.	15.12%	13
Es una alternativa tecnológica más para procesar los datos eficientemente.	74.42%	64
No asegura la eficiencia en el procesamiento eficiente de los datos.	10.47%	9
TOTAL		86

los datos IoT cerca de los dispositivos que producen y actúan sobre los mismos, es decir, mediante la arquitectura de computación en la niebla.

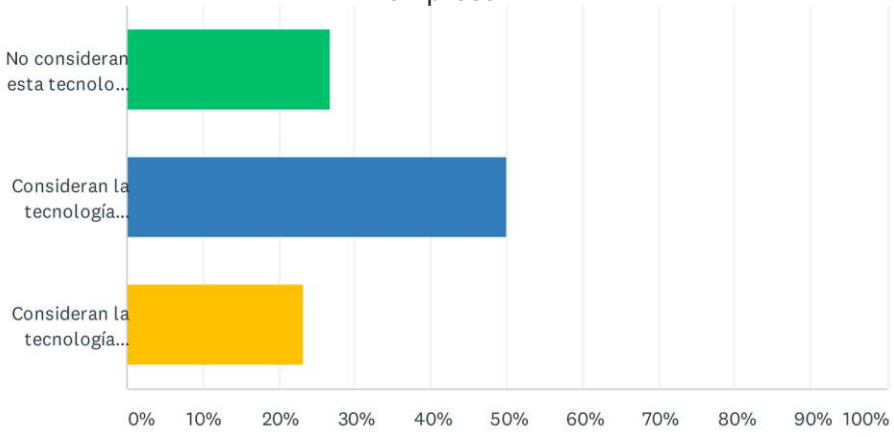
Estas posibles ventajas que otorga el procesamiento en la niebla o en el borde, parecen reconocerse según los resultados de la encuesta que advierten confianza en estas arquitecturas computacionales, otorgando un 74.42% como una alternativa tecnológica más para el procesamiento de los datos, y un 15.12%, lo visualiza como la alternativa ideal. Así, solo un 10.47% manifiesta escepticismo frente a su eficacia en el procesamiento de los datos. Una vez más, se vislumbra una oportunidad para la apropiación futura de estas tecnologías, con un 89.54% de reconocimiento de su eficacia (Ver Figura 5).

Pregunta 6: Percepción de las empresas acerca de la adopción de la tecnología de *Computación en el borde*

El "*hype cycle"* o "ciclo de sobreexpectación" creado por la consultora tecnológica Gartner constituye una herramienta muy reconocida para comprender el proceso de introducción de las innovaciones preferencialmente tecnológicas, en el mundo empresarial y de negocios.

Su pronóstico sobre la inmersión de la *Computación en el Borde*, responde positivamente a la expectativa que suscita el uso de la com-

Figura 6. La consultora Gartner estima que en 2025 el 75% de los datos empresariales se procesarán en el borde, en comparación con el 10% actual. Este pronóstico plantea una alta inmersión en el entorno empresarial de este enfoque tecnológico. En su caso, los directivos de su empresa:



OPCIONES DE RESPUESTA	RESPUESTAS	
No consideran esta tecnología relevante para las actividades de la empresa.	26.74%	23
Consideran la tecnología relevante pero su implementación viable sólo en el largo plazo.	50.00%	43
Consideran la tecnología relevante y contemplan su implementación en el corto o mediano plazo.	23.26%	20
TOTAL		86

putación en la nube, en ciertas aplicaciones, primordialmente en lo relacionado con la latencia, el procesamiento distribuido y la seguridad de los datos.

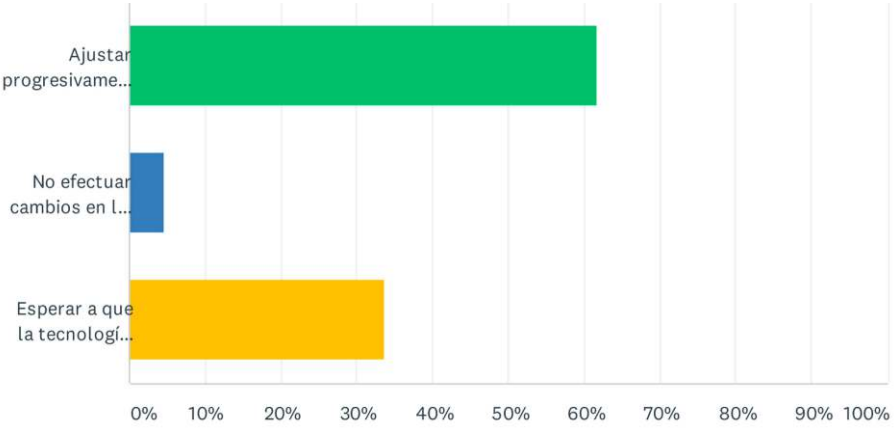
Los resultados permiten identificar el reconocimiento de la relevancia de la *Computación en el Borde*, por parte de las empresas y expertos de TI, con un 73.26% en total, visibles en la Figura 6; no obstante, casi dos terceras partes de ellos, la perciben viable sólo en el largo plazo. Esto revela una demanda por mayor formación de expertos en estas tecnologías, y la necesidad de contar con más casos de uso significativos que permitan evidenciar el apalancamiento de las empresas a partir del uso de estas tecnologías.

Debe mencionarse también ese 26.74% que no considera estas tecnologías relevantes para su empresa, explicable en la idea de que no existe nada posible en el borde, que no se pueda realizar también en la nube. Quizás la respuesta sea obvia para empresas de sectores como la manufactura, en la que una latencia de milisegundos para tomar una decisión puede ser determinante, pero es cierto también que hay decisiones que soportan los tiempos de respuesta que ofrece la nube.

Pregunta 7: Proceso de adopción de la Computación en el Borde y en la Niebla en las empresas

Cuando en 1979 Alvin Toffler anunció en su libro[2], la inminencia de la

Figura 7. Considerando el efecto de la adopción de la computación en el borde y en la niebla sobre la arquitectura de las aplicaciones, las empresas que tienen aplicaciones basadas en la nube deberían:



OPCIONES DE RESPUESTA	RESPUESTAS	
Ajustar progresivamente estas aplicaciones para aprovechar los beneficios del cómputo en el borde.	61.63%	53
No efectuar cambios en las aplicaciones para evitar los riesgos de seguridad asociados con el nuevo enfoque.	4.65%	4
Esperar a que la tecnología de computación en el borde y la niebla, tenga un uso más generalizado para hacer cambios.	33.72%	29
TOTAL		86

tercera ola con cambios significativos en diversos ámbitos de la vida humana, basado en una revolución de las TICs, con un sistema de producción basado en la información, medios de comunicación globalizados, interactivos y colaborativos, probablemente contribuyó a prepararnos para el cambio, pero quizás no, para la velocidad y contundencia con la sobrevendrían las siguientes olas.

El final del siglo XX y las dos primeras décadas del XXI, han enfrentado a los tomadores de decisiones en las organizaciones a cambios continuos y a tecnologías disruptivas que desafiaron sus sistemas, procesos y paradigmas.

Las respuestas de los encuestados frente al proceso adecuado de sus empresas para adoptar la *Computación en el Borde y en la Niebla* revelan una posición de cautela, representada en un 66.63% que considera que se debe llevar a cabo un ajuste progresivo de las aplicaciones, más un 33.72% que preferirían esperar a que estas tecnologías tengan un uso más generalizado antes de hacer cambios (Ver Figura 7).

De nuevo se requieren más casos de uso que puedan evidenciar las ventajas reales de estas tecnologías y su potencial para incrementar la competitividad de las empresas.

Pregunta 8: Compromiso con la seguridad de los datos en los servicios en el borde, debido al alto número de dispositivos (IoT)

Con una arquitectura IoT, los servicios en el borde suponen el procesamiento de los datos, incluso en los mismos dispositivos, y exige por tanto garantizar su inteligencia y autonomía, además de dotarlos de microcontroladores para dicho procesamiento y para poder "hablar" con otros dispositivos locales o externos.

Este escenario, sin embargo, implica un esfuerzo por parte de los directivos para proteger los sensores y dispositivos ante fallos o amenazas o intrusiones que pueden poner en riesgo no solo los datos, en muchos casos datos sensibles, sino también la correcta ejecución del sistema.

Es por ello comprensible la posición de los encuestados, de los cuales un 72.09% (Ver Figura 8) ve comprometida la seguridad de los datos al utilizar servicios en el borde.

No obstante, un 27% no encuentra este tipo de problemas y los análisis aquí pueden variar desde un verdadero desconocimiento de dichos riesgos o amenazas o bien, con una visión más optimista, a par-

[2] TOFFLER, Alvin. La Tercera Ola, 1993. – Plaza & Janes

tir de experiencias exitosas con el uso de servicios en la nube, la niebla o incluso en el borde mismo.

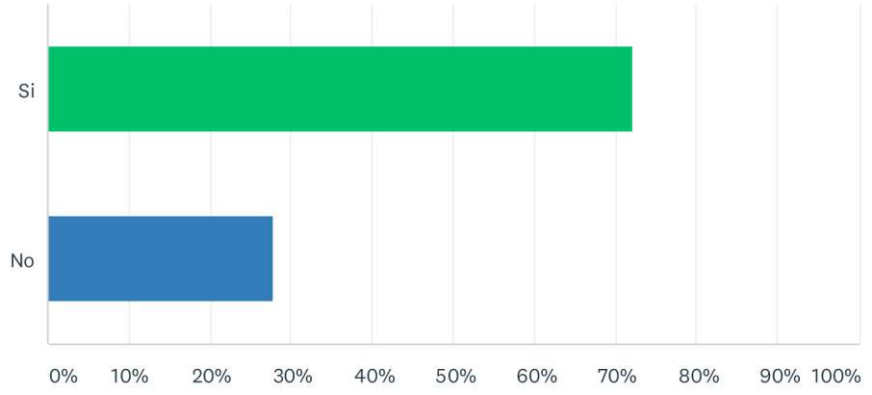
Pregunta 9: Riesgos de seguridad más relevantes identificados por los servicios en el borde

Los riesgos de seguridad en el uso de servicios en el borde que más preocupan a los ingenieros y expertos de TI, están claramente asociados con la confidencialidad de los datos. Un 78.82% de los encuestados, prioriza este aspecto, aunque un 44% también encuentra amenazas a la seguridad por pérdida de integridad y un 37.65% por pérdida de disponibilidad, como se observa en la Figura 9. En este sentido, a pesar de que muchos manifestaron en respuestas previas el desconocimiento y otros la falta de comprensión de estas tecnologías, existe un acierto al visualizar amenazas en estos 3 aspectos, sobre los cuales la mayor inmersión en uso de servicios en el borde, deberá dar respuestas a directivos y líderes de TI que eleven la confianza de los usuarios y permitan que más usuarios acojan esta nueva ola tecnológica.

Pregunta 10: Percepción sobre apalancamiento de la *Computación en el Borde* y en *la Niebla*, para la adaptación de las empresas al contexto digital

Siendo ésta una pregunta abierta, pueden resumirse las respuestas en una mayoría que la encuentra atractiva y le concede posibilidades para apoyar la resiliencia de las operaciones de las empresas, pero con salvedades garantizar la segu-

Figura 8. ¿Considera usted que la seguridad de los datos se verá comprometida al utilizar servicios de cómputo en el borde, teniendo en cuenta el alto grado de proliferación de dispositivos conectados en las empresas y en los hogares (IoT)?



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	72.09%	62
No	27.91%	24
TOTAL		86

ridad de los datos, o la comprensión del "tiempo real" que no siempre es real, sino cercano al real, dependiendo del tipo de sistema o empresa.

Sin embargo, algunos la encuentran muy atractiva, considerando las circunstancias que enfrentó el planeta en el presente año, con exigencias de conectividad y comunicación efectiva en las corporaciones, en entornos netamente digitales.

Cabe señalar un grupo menor de respuestas que se acogen a modelos más conservadores, los cuales suponen gestionar los datos a nivel local o bien el uso de la nube, con servidores que respondan a sus servicios de computación, sin poner en riesgo la seguridad de sus datos.

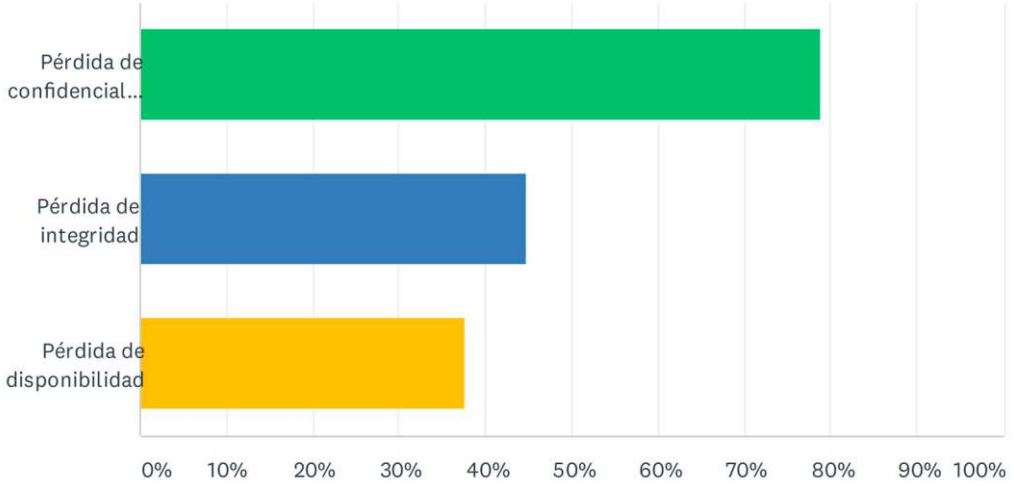
Hay bastante franqueza en algunas respuestas sobre el desconocimiento de este impacto, manifiesto en forma explícita o por la omisión en la respuesta.

Conclusiones

Esta investigación permite formular algunas conclusiones, relacionadas a continuación:

- Se requieren mayores esfuerzos para que los directivos y expertos en TI conozcan y entiendan estas tecnologías, idealmente con la ilustración a través de casos de uso significativos, que in-

Figura 9. Si la respuesta es afirmativa, qué riesgos de seguridad identifica como los más relevantes: (señale todos aquellos que apliquen).



OPCIONES DE RESPUESTA	RESPUESTAS	
Pérdida de confidencialidad	78.82%	67
Pérdida de integridad	44.71%	38
Pérdida de disponibilidad	37.65%	32
Total de encuestados: 85		

crementen su confianza y evidencien su potencial en cuanto a procesamiento eficiente y ventajas competitivas para las organizaciones.

- Si bien las alternativas de procesamiento en el borde en un entorno IoT, ofrecen respuestas en cuanto a la velocidad de respuesta, la seguridad de los datos y la eficiencia del procesamiento, persiste escepticismo en los usuarios atinentes a la confidencialidad, la disponibilidad y la integridad de los datos.

- La velocidad de cambio de las tendencias tecnológicas, desafía los ciclos de evolución y maduración de los sistemas de información y plantea retos a directivos y tomadores de decisiones, con tecnologías disruptivas que permean los paradigmas organizacionales, con alternativas a veces no consolidadas o suficientemente probadas.

Libia Denisse Cangrejo Aljure *Ingeniera de Sistemas, PhD en Ingeniería – Sistemas y Computación y Msc. en Geomática, de la Universidad Nacional de Colombia. Especialista en Teledetección, Cartografía y SIG de la Universidad Alcalá de Henares, España y especialista en SIG, de la Universidad Distrital Francisco José de Caldas. Desarrolló su tesis doctoral en el campo de Modelado Semántico de Contexto para el ámbito de Internet de las Cosas, con Linked Open Data. Docente de la Facultad de Ingeniería de la Universidad Nacional de Colombia. Ha participado y liderado proyectos de TI y Geoinformación en diversos campos, algunos de ellos de carácter social, como El SIG de Gestión Local para Ciudad Bolívar, en la Corporación SUR, Georreferenciación y Reingeniería para la Gestión del Conflicto Local de la Candelaria, Diseño conceptual del SIG para la Mesa Regional de Planeación Bogotá–C/marca, PNUDR/UNAL y el Convenio UNAL/MinTIC, Computadores para Educar, entre otros.*

Computación en el borde y en la niebla, tendencias e inmersión

DOI: 10.29236/sistemas.n156a5

El tema seleccionado mucho antes de la pandemia para esta edición resulta de gran envergadura, considerando la multiplicación de dispositivos conectados.

Sara Gallardo M.

Cuando aparecieron los conceptos de computación en el borde y en la niebla (*Edge y Fog Computing*), en referencia a la estructura de redes y a la información circulante en múltiples dispositivos relacionados con Internet de las Cosas (IoT), lejos estaba la humanidad de imaginar la multiplicación billonaria de aparatos conectados y más lejos aún, de que la pantalla de un computador fuera protagonista en los hogares del mundo.

La pandemia ocasionada por el COVID-19 ubicó los desarrollos tecnológicos como prioridad entre las necesidades básicas de los seres humanos, especialmente insatisfechas en los países tercermundistas.

De 500 millones de dispositivos conectados en 2003[1], hoy se habla de 30.000 millones por obra y gracia del coronavirus, sin contar la población más desprotegida y sin recur-

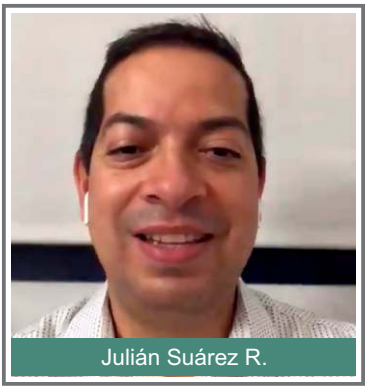
sos para adquirir un equipo de computación[2].

De ahí la relevancia de reunir voces especializadas para analizar distintos aspectos sobre la computación en el borde y en la niebla. A la cita virtual acudieron: Felipe Nicolás Diniello, Iot Engineer de Globant; Juan Francisco Jurado Páez, Consultor Senior IoT de Globant y Julián Suárez Ramírez, Consultor Senior de IoT en AWS Professional Services en Amazon.

"Esta temática es de frontera y nos permite mirar el mundo en una interconectividad abierta y avanzada, con base en los nuevos desafíos de los desarrollos tecnológicos", manifestó Jeimy J. Cano Martínez, director de la revista.

Por su parte, Denisse Cangrejo Aljure, moderadora del encuentro, agradeció a los invitados por su presencia y agregó: "este espacio proporcionado por la Asociación Colombiana de Ingenieros de Sistemas, (Acis), es muy importante para que los ingenieros nos sintamos parte de este grupo a nivel nacional" y entró de lleno al debate formulando la primera pregunta:

[1] https://www.xataka.com/internet-of-things/edge-computing-que-es-y-por-que-hay-gente-que-piensa-que-es-el-futuro. Recuperado julio 30 de 2020.
[2] https://asiet.lat/actualidad/entrevistas/el-papel-que-jugara-el-internet-de-las-cosas-despues-de-la-pandemia/. Recuperado agosto 3 de 2020.

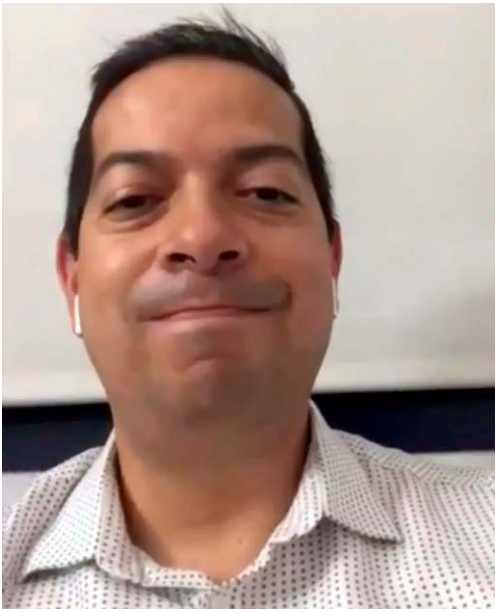

Julián Suárez R.


Felipe Nicolás Diniello


Juan Francisco Jurado P.

En el entorno de Internet de las Cosas, ¿qué es la computación en el borde y en la niebla?, ¿cuáles son sus diferencias y qué beneficios ofrecen a los desarrolladores de software?

Julián Suárez R.
Consultor Senior de IoT
AWS Professional Services
Amazon



Aunque la pregunta es muy interesante puede resultar confusa, dependiendo a quién se le dirija, si a los ingenieros, a las empresas, a la academia o al sector de tecnología. Desde mi perspectiva, no existe distinción entre computación en el borde y en la niebla. Lo que podría decir al respecto es sobre las ventajas, y aunque las empresas no están muy acostumbradas a estos conceptos, suelen manejarlo sobre lo trabajado localmente *On-Premises* y posteriormente enviarlo a la nube. Precisamente, ahí es en donde se encuentran el borde y la niebla para realizar la conectividad con el procesamiento de datos en la nube, optimizar el envío de datos para los dispositivos con menos ancho de banda, controlar dispositivos remotos con difícil acceso a Internet y utilizarlos para disponer de redes interconectadas, todo en dirección a la nube. Con relación a las diferencias, cuando en *Edge Computing* nos referimos a un dispositivo en particular que ayuda a la conexión en la nube, mientras que *Fog Computing* facilita la comunicación de estos dispositivos en relación directa con la nube. La gran diferencia la resumo en que *Edge* es un dispositivo en particular y *Fog* se refiere a la red de conexión de dispositivos hacia la nube. Esto dependerá, por supuesto, de la infraestructura y de las redes de comunicación que utilicemos. Para citar un ejemplo, no es tan fácil en una solución de *Smart City* conectar todos los semáforos de la ciudad, considerando que no en todos los lugares en donde están ubicados es posible disponer de *wifi* o 4G; muy distinto a lo que sucede en una empresa, en la que todo está muy bien conectado. Así mismo, en una fábrica de manufactura en la que se puede ofrecer interconectividad vía *Ethernet* o *wifi* a los dispositivos.

Insisto en que, si estos conceptos de computación son manejados entre las personas, la percepción difiere a la de una empresa, am-

biente en el que todo está perfectamente controlado.

Felipe Nicolás Diniello
IoT Engineer
Globant

Existe una similitud muy grande entre *Edge* y *Fog Computing*, basada en que hay mucho dispositivo por fuera de *cloud computing*. Contamos con una solución en un servidor, pero normalmente está concentrado, lo que no sucede con los primeros que funcionan en la periferia y el usuario tiene contacto entre los diferentes puntos. Y la principal diferencia entre Edge y Fog es que en esta última tecnología hay una comunicación transversal entre los mismos puntos, mientras que en Edge, aunque pueda existir la misma transversalidad en la comunicación o no, se da un procesamiento adicional in situ; es decir, hay un *hardware* específico haciendo procesamiento de señales en tiempo real y sólo comunica un evento asociado a detectar o, por ejemplo, en el caso de procesamiento de video en tiempo real, que de ahí sólo se transmite un evento detectado en vez del video en sí.

Juan Francisco Jurado P.
Consultor Senior IoT
Globant

Antes que citar una diferencia puntual, quiero hacer una comparación en tiempo. En el año 2003, los dispositivos que conectaban a una persona se reducían a uno; representados en cifras en 0.08 dispositivos, de acuerdo con la información suministrada por McKinsey, en abril de 2011. Hoy, en 2020, la investigación más reciente refleja 6.6 dispositivos conectados por persona, es decir, un incremento superior al 600%. Lo que quiere decir que los desarrollos tecnológicos deben cambiar en forma exponencial. En otras palabras, debe existir mayor capacidad de procesamiento de datos, mayor captura de los mismos y, sobre todo, se abre el espectro para pensar en qué hacer con esos datos. De ahí salen términos relacionados con inteligencia artificial, un poco más sofisticados. En palabras muy coloquiales, la idea es que *Edge Computing* permite que los datos producidos por un dispositivo estén justo en el lugar en donde el *hardware* ha sido puesto en marcha. La idea es separar un poco el *cloud computing* y llevar ese procesamiento lo que

más se pueda en tiempo real; aunque todavía esto no es del todo posible, lo será más rápido de lo que se cree y más eficiente.

Denisse Cangrejo A.

En las últimas décadas, algunos desarrollos fueron determinantes para la computación del siglo XXI: la creación de Internet a partir de ARPANET (1962), el desarrollo de sistemas operativos multiusuario con Unix (1969), la creación de la World Wide Web en el seno del CERN, propuesta por Tim Berners-Lee (1989-1991); los sistemas operativos como Windows de Microsoft y luego sistemas operativos abiertos y gratuitos como Linux (1991). Todos ellos dieron paso a esta confluencia tecnológica actual sobre la cual se asienta Internet de las Cosas. ¿La pregunta es si ustedes consideran que la computación en el borde y en la niebla se perfilan en el horizonte cercano como desarrollos que trascenderán el momento actual y harán viable esa ingente cantidad de aplicaciones con el sello de "inteligencia" que promete Internet de las Cosas?

Felipe Nicolás Diniello

Esto es una promesa que viene ocurriendo hace mucho tiempo. Hoy en día y, cada vez con más en auge, la curva de dispositivos es exponencial, estamos en un punto de inflexión, directamente relacionado con el desarrollo de *h*ardware, de donde resulta Internet de las Cosas. En mi calidad de ingeniero electrónico es asombroso observar cómo en menos de 10 años se ha dado una explosión tecnológica; el hardware disponible era mucho más difícil de obtener, más costoso y complicado para usar, de lo que se ve hoy en día. Cualquier adolescente con muchas ganas alrededor de la tecnología y desde su casa puede enviar un montón de información con apenas unos pocos dispositivos, que no existían en mi época universitaria. Todo eso se fue dando por el abaratamiento de los costos en los desarrollos tecnológicos y de los servicios que se ofrecen a su alrededor. Disponer hoy de un microcontrolador que se conecta a internet cuesta centavos de dólar. Se lleva a casa para empezar a trabajar. En otras palabras, el desarrollo de hardware generó tales cambios en muy corto tiempo. De manera que en el presente es posible generar sus propios avances para entrar en una etapa productiva. Existe una cuestión diferente entre lo que es una posibilidad a través de Internet de las Cosas y un desarrollo web clásico, que no se ve en una aplicación de software puro. El hardware y sus desarrollos ayudaron a pavimentar ese camino y ahora estamos más cerca de cumplir esa promesa.

Juan Francisco Jurado P.

Sin duda alguna sí se ve en el horizonte. Ya no hablamos de un futuro cercano, porque lo estamos viendo en este presente. Lo han marcado en un gran concepto que podría sonar un poco cliché, la Revolución de la Industria 4.0. Muchas de es-

tas tecnologías venían existiendo, la gran pregunta es ¿cuál es el boom? Básicamente, por la masificación de los dispositivos y de la conectividad disponibles en una aplicación final. Empresas líderes en Internet de las cosas invierten millones de dólares en *Edge* y *Fog Computing*, tecnologías aplicables en diversas áreas de la industria, del conocimiento y hasta en la educación. Hoy en día vemos robots domiciliarios. Así mismo, estamos conectados en forma segura, los usuarios corrientes a más de tres o cuatro dispositivos y los aficionados a la tecnología como yo, disponemos hasta de 15 dispositivos o más en conexión. Es nuestra realidad en medio del cambio y entre la pandemia. Se trata de darle la bienvenida a todo esto que está ocurriendo.

Julián Suárez R.
Mi postura no difiere mucho de lo ya expuesto. Todos estos eventos como la aparición de Internet y lo demás han sido hitos definitivos para la humanidad. Desde hace más de 10 años ha habido una evolución y surgimiento de otras alternativas que nos permiten conectar los diferentes dispositivos. La tecnología seguirá avanzando a un ritmo bastante rápido, que nos lleva a ver el ambiente de la nube −que todo el mundo ya utiliza−, como una opción para conectar billones de dispositivos, pero en forma local, en donde entran en juego *Edge* y *Fog Computing* para contribuir con la inteligencia artificial y no tener que esperar a la respuesta de los datos enviados a la nube. Todo acompañado de la evolución en *hardware* y *software*, microcontroladores a bajo costo con diseños diferentes a las cajas enormes de otros tiempos. Y a nivel de los desarrolladores significa no estar utilizando solamente lenguajes de otras épocas, que sólo entendían ciertas máquinas, sino lo que se puede hacer ahora con otras herramientas para diferentes tipos de *hardware* en el marco de *IoT*.

Denisse Cangrejo A.
La práctica de los ingenieros de sistemas y computación está claramente asociada al desarrollo tecnológico y la computación en el borde y en la niebla son una evidencia de ello. Según sus conocimientos y experticia, ¿qué opinan respecto a la posibilidad de privilegiar en el ingeniero de sistemas, la capacidad de aprender a aprender, por encima del aprendizaje mismo de tecnologías?

Juan Francisco Jurado P.
“Nunca pares de aprender” es una frase motivadora de Fredy Vega, CEO de Platzi, que nos debe estimular y en mi caso particular es un modo de vida. El mundo está cambiando exponencialmente en todas direcciones y más en asuntos tecnológicos. Hace 40 o 50 años los profesionales se especializaban en algo muy puntual y esta tecnología permanecía por un tiempo largo, cosa que no sucede hoy en día, en que lo aprendido, al cabo de un año

ya es obsoleto y la mayoría de asuntos no se usan; por tal razón, es necesario un cambio de mentalidad en los estudiantes del presente. El sentido de asistir a la universidad contempla adquirir la capacidad de asumir retos en la vida de carácter tecnológico; en la capacidad de asimilar un conocimiento nuevo y de modificar las visiones personales para atender el auge tecnológico. Además, de revisar la especialización del trabajo. Hoy contamos con profesionales dentro de una especialidad en cada parte de la torta del desarrollo. Antes, el ingeniero de sistemas era el responsable de todo, entre mantenimiento, operatividad y procesos, entre otros aspectos. Eso ya no existe por los cambios en la tecnología y por las nuevas posiciones basadas en la especialidad, cada vez más específica, para el funcionamiento diario de las empresas.

Julián Suárez R.

No es fácil la respuesta; en mi caso, a pesar de que me gusta mucho la academia, no estoy muy familiarizado en la creación de programas estudiantiles. Pero, de acuerdo con mi experiencia personal lo que se necesita es recibir unas bases que den lugar a ese raciocinio para no quedarse solamente con lo aprendido en la universidad. Tales bases deben generar otros aprendizajes y nuevos lenguajes de programación. Se tiene que llegar a la creación de las bases para desarrollos como los que estamos tratando en esta reunión. Con las redes 5G y demás se producirán muchos cambios. Aún así, se deberían incluir temas en esa dirección. Con relación a “nunca parar de aprender”, en Amazon tenemos un principio de liderazgo “aprende y sé curioso”, en otras palabras, la curiosidad puesta en práctica para descubrir nuevas formas de hacer las cosas, de atacar los problemas de manera diferente.

Felipe Nicolás Diniello

Durante mucho tiempo fui docente en la universidad y, desde luego, la academia me motiva mucho. Es muy importante tener en cuenta que la tecnología cambia, pero los conceptos no, pueden cambiar las formas, pero las bases son las mismas. Hoy en día recurrimos a la abstracción en muchos asuntos. Todo lo relacionado con la tecnología será siempre cambiante. La docencia está orientada a formar profesionales en conceptos que puedan servir a la industria, formación basada en las tecnologías del momento para que los profesionales la puedan entender. Lo que vemos, por ejemplo, con C++, tecnología de hace muchos años, herramienta vital para muchos. Hoy tenemos lenguajes más modernos sobre una misma base, el concepto es el mismo. De esa forma el alumno saldrá a la industria a seguir aprendiendo, pero contará con las bases necesarias para saber cómo seguir actuando. En el ámbito académico no es fácil estar introduciendo reformas al plan de enseñanza, pero es necesario hacerlo. Está bien que

la enseñanza continúe con las bases, pero también es urgente la actualización hacia el cambio.

Denisse Cangrejo A.

Uno de los mayores retos que Internet de las Cosas plantea a las redes de comunicación es el nivel de rendimiento asociado a la latencia, la velocidad de los datos, el consumo de energía y el número de dispositivos que soportan. Las redes 5G ofrecen una infraestructura prometedora en este sentido para el desarrollo de IoT. ¿Cómo evalúan ustedes la integración de la computación en la niebla y en el borde para el desarrollo de aplicaciones IoT con la quinta generación de redes inalámbricas?

Julián Suárez R.

Efectivamente, las redes 5G están causando y lo seguirán haciendo un gran impacto positivo hacia los problemas de comunicación que queríamos resolver, en forma específica en el envío de videos de cámaras o grandes volúmenes de datos hacia la nube o hacia otros dispositivos. Al tener una red de alta velocidad podremos enviar mayores datos a la nube y, por tanto; pero, siempre habrá que identificar el criterio sobre cuáles datos quiero enviar y si debo esperar una respuesta o no para ejecutar una acción en el borde. Esto tiene todos los retos de implementación y al final serán otra opción muy buena para conectar los dispositivos, pero tampoco quiere decir que, si tenemos soluciones para agricultura sin posibilidades de tecnologías 5G, el trabajo no se podrá hacer, para eso existe otro tipo de redes que permite hacer realidad el *IoT* en estos escenarios. Otros fabricantes facilitarán ubicar antenas, llegar a un concentrador para enviar a la nube los datos. Esto nos va a ayudar mucho, la evolución seguirá. Se trata de poder tener comunicación más rápida, más efectiva, alrededor de dispositivos en tiempo real. El *boom* de Internet de las cosas crecerá en estos tipos de red con una conectividad completa.

Felipe Nicolás Diniello

Lo más importante es hablar de las opciones. Hoy vemos a 5G como la gran alternativa en IoT, pero la gran promesa está basada en la cantidad de dispositivos y el ancho de banda disponibles, aspectos que no bastan. La realidad es que las grandes ciudades tendrán grandes posibilidades de comunicación con muchos beneficios en el marco de una infraestructura muy sólida. No obstante, en las ciudades pequeñas y áreas remotas persistirán las dificultades de comunicación. Algunas aplicaciones para la agricultura están a kilómetros de la antena de cubrimiento de redes más cercanas, así que cualquier solución se dificultará. Pensar en 5G solamente no es suficiente, en la medida en que existen otras tecnologías como *LoRA Wan* y *Narrow Band IoT*, para situaciones remotas y de muy bajo consumo, 14 o 20 kilómetros con consumo de batería ínfimo y muy sólidas en cubrimiento. En esa

dirección hay muchas opciones de conectividad. En *Edge* y *Fog computing* se está hablando de la transversalidad en la comunicación entre dispositivos tipo Mesh, para hablar de otras topologías de redes y de ambientes más lógicos y más fáciles. 5G es una tecnología muy prometedora, pero es necesario pensar en otras opciones.

Juan Francisco Jurado P.

De acuerdo con todo lo aquí expuesto; la integración de *Edge Computing* bajo la premisa de 5G es interesante, pero esto no será la panacea; es posible que se aumenten los dispositivos de conexión. En el marco de los carros autónomos, 5G sí tiene una amplia importancia, en la medida en que ofrece mayor velocidad en la transmisión de datos y menos latencia, ventajas que son muy importantes. Menciono el caso de uso exitoso en que 5G puede descifrar para convertir la movilidad de una ciudad, por ejemplo, en forma autónoma; comunicar carros entre ellos sin ir a *cloud* de forma muy rápida y eficiente. Se trata de un asunto de comunicación de la ciudad con los autos. Es un caso de uso muy exitoso que puede llegar a masificar el gran *boom* de los carros autónomos, un sector entre internet de las cosas e inteligencia artificial, una mezcla entre las dos tecnologías.

Denisse Cangrejo A.

¿Más ampliamente, podríamos decir que 5G se convierte en un habilitador de Fog y Edge computing? ¿Más para unas aplicaciones que para otras?

Felipe Nicolás Diniello

De acuerdo. Es un habilitador para algunas, para la gran mayoría es una opción más. Pero hay asuntos no viables para ese tipo de comunicación.

Denisse Cangrejo A.

La computación en el borde extiende los servicios de la nube para proveer recursos computacionales en el borde. Sin duda, eso implica un beneficio, pero también se adivinan riesgos de seguridad de los datos que se generan en los dispositivos y requieren estar protegidos en los tres niveles. Quisiera conocer su percepción con respecto a la seguridad y a la privacidad de los datos IoT y las alternativas de gestión que pueden ofrecer protección a los mismos.

Felipe Nicolás Diniello

Desde el punto de vista de seguridad cualquier plataforma de IoT ofrece muchísimas alternativas para la gestión de claves y accesos, ya sea con servicios de encriptación o por medio de certificados pre-compartidos. Muchas de las herramientas de IoT ya tienen módulos para vincular y desvincular dispositivos como solución a cualquier problema. En lo relacionado con el transporte de los datos se buscan alternativas para que los dispositivos no almacenen las claves, sino que las gestionen a través de servicios de provisioning para que puedan ser renovadas, así como también implementar Listas Blancas o Negras para dispositivos. En términos de seguridad no hay muchos inconvenientes, toda vez que se trata de las mismas tecnologías en uso. Una vez que los datos están en la nube, surge el tema de la privacidad, durante toda la etapa de transporte está garantizada, pero pasa a ser ciento por ciento de la empresa o el servicio que facilita el uso de los datos, en torno al contrato legal acordado. La privacidad es un asunto que desde nuestra perspectiva tecnológica no está tan comprometida, es un tema de negocio.

Julián Suárez R.

La seguridad es uno de los principales asuntos que se deben tratar en cualquier sistema o solución, siempre es importante. A través de la historia nos hemos dado cuenta de los errores cometidos, en el sentido de que, por el afán de habilitar servicios, olvidamos la seguridad. De ahí que, en los últimos años, la denegación de servicio ha obedecido precisamente a dispositivos IoT, cámaras, webcam, entre otros. En el afán por poner en marcha e implementar el servicio, el error humano está presente. Existen dispositivos para controlar la seguridad, pero es necesario contemplar las opciones en ese ambiente. Hay varias técnicas como cifrado de punto a punto, cifrado de los datos en el borde y la niebla, así como en la nube, además de apoyarse también en los mecanismos de seguridad habilitados en los dispositivos, encaminados a eliminar los huecos de cara a la seguridad. El afán de salir al mercado con un producto afecta la seguridad. En cuanto a la privacidad depende de esos acuerdos firmados, un asunto muy en auge hoy, que depende de las leyes de cada país. En Europa existe GDRP para que los datos no sean tratados

con la libertad tradicional, de manera que la captura de datos esté cobijada. Se trata de disponer de tecnología soportada en la regulación necesaria.

Denisse Cangrejo A.
¿Los riesgos aumentan en el borde y en la niebla, más que en la nube?

Julián Suárez R.
No creo, los mecanismos de seguridad existen para su implementación. En la nube nosotros manejamos el concepto de responsabilidad compartida, lo que significa que en la infraestructura proporcionamos todos los mecanismos de seguridad adecuados, pero, a nivel de los servicios y los datos, el cliente es el responsable de habilitarlos. En la medida en que la nube soporta a varios clientes, se piensa que el riesgo es mayor y puede recibir ataques diferentes que afectan gravemente la seguridad, pero, como he mencionado antes, la responsabilidad compartida es esencial para que no sean efectivos dichos ataques. No creo que sea inseguro, siempre y cuando sean aplicados los principios de seguridad. Esto no solo sucede en el caso de IoT; por ejemplo, para un banco o un portal transaccional, si no se piensa desde el día primero se registrarán problemas de seguridad.

Juan Francisco Jurado P.
Difiero un poco en tal sentido, porque entre más puntos de procesamiento de datos o transmisión de datos, existe el riesgo de ataque. Las empresas grandes que se preocupan por la seguridad en *cloud* son *Amazon*, *Microsoft*, entre otras; son compañías que han abierto su portafolio, incluso a seguridad para este tipo de zonas. La pregunta puntual es si se puede llegar a estar más afectado solo por el hecho de que empiezan a descentralizar procesos y dispositivos; por probabilidad se aumentan los puntos de riesgo. El otro punto de vista tiene que ver con que todos los dispositivos conectados están adquiriendo información en forma permanente, están relacionados con temas como temperatura, productos y otros. Inclusive, se habla de que la voz es grabada. Se trata de un cambio de mentalidad y de inmersión tecnológica. Personalmente, estoy a favor de que me rastreen porque eso hace que mi vida sea más interesante, más divertida. Si *Facebook* me rastrea en mis compras, podrá mostrarme lo que me pueda interesar, sin que yo haga la búsqueda. *Google* puede conocer los gustos de los usuarios en diferentes asuntos. Por ejemplo, cuando se trata de viajes, esta compañía puede organizar una sorpresa con base en esos seguimientos. Esto puede representar una experiencia diferente para las personas, y puede significar 'ponerle la fresa al pastel' en estos temas que estamos tratando. Con relación a los datos pueden verse más afectados, pero tecnológicamente no, en la medida en que muchas empresas están produciendo mecanismos de ciberseguridad,

además de mantenerlos bajo mecanismos de protección. En mi concepto, se trata de un gana-gana en términos tecnológicos. En *Google maps* pueden observar el mapa de sus movimientos diarios. Si esa información cae en malas manos, pues es un riesgo, pero está en manos de la empresa que gestiona ese tipo de datos y que debe responder por los mismos.

Denise Cangrejo A.

Esa posición relacionada con la privacidad reta algunos de mis paradigmas, la juventud lo ve de manera distinta. Me gustaría conocer la opinión de los otros panelistas al respecto.

Jeimy J. Cano M.

Esa es mi especialidad con más de 24 años trabajando los temas de seguridad y privacidad. La computación en el borde (*Edge*) y en la niebla (*Fog*) aumentan la superficie de ataque por la cantidad de puntos de conexión expuestos. El asunto es la capacidad de la empresa para poder brindar una seguridad transversal a sus clientes. Por otra parte, los dispositivos son ahora cada vez más pequeños y cuentan con microcódigo en el firmware, que con el paso del tiempo tendrán que actualizarse, lo que se traduce en nuevos puntos de acceso y vulnerabilidad. Los atacantes pueden enviar a los usuarios actualizaciones maliciosas y aprovechar tales circunstancias para violentar la seguridad y privacidad. Asuntos como estos son escenarios ya planteados en la industria que retan los modelos de seguridad y control.

Ahora en este ambiente más distribuido los conceptos de seguridad tienen que cambiar. En este sentido, la seguridad requerirá analítica de comportamientos con relación a los dispositivos e inteligencia de amenazas como la base de sus nuevos fundamentos.

Felipe Nicolás Diniello

La superficie de ataque se amplía lo que lleva a considerar cómo empezar a hacer inteligencia artificial sobre estos volúmenes de información para generar lo que podríamos denominar un anticuerpo y controlar la situación. En el nuevo panorama tenemos una célula compuesta por una serie de diferentes dispositivos en el borde, que requieren la generación de esos

anticuerpos para cubrirla y protegerla en dirección a combatir el comportamiento anómalo o dispositivos comprometidos. Se trata de una burbuja que exige un tratamiento cuidadoso, con nuevas herramientas de defensa.

Juan Francisco Jurado P.
En mi opinión sugiero que cuando descarguen alguna aplicación den vía libre a compartir todo.

Denisse Cangrejo A.
¿Cuáles consideran que son los retos mayores que deberá asumir el sector empresarial para la apropiación de las tecnologías Edge / Fog Computing en el futuro cercano? ¿En qué aspectos no se puede equivocar la industria en la apropiación de esas tecnologías?

Felipe Nicolás Diniello
Hay dos aspectos relacionados con la adopción de estas tecnologías. Por una parte, las empresas que brindan los servicios en comunicaciones y todo lo relacionado con *Edge Computing* y las buenas prácticas desde el punto de vista de seguridad. Es necesario hacer las inversiones correspondientes para su adopción. Desde el punto de vista del usuario, tienen que asumir el cambio de paradigma. Nos sucedió en soluciones monolíticas, es decir, el servidor con todo. Y el nuevo paradigma se traduce hoy en un *Fog* que exige un cambio de mentalidad, frente a los diferentes componentes del ecosistema, aspecto muy difícil.

Julián Suárez R.
En mi opinión, el gran reto en el sector empresarial está en cómo romper esa cultura que lleva a sus empleados a salir de su área de confort para implementar algo nuevo como *Edge* y *Fog*, que contemplan la llegada de nuevos dispositivos y puntos de conexión. Esto es complicado en las empresas, pero es necesario hacerlo. Descubrir los mecanismos adecuados para el cambio, algunos de ellos mostrando el beneficio, mayores ingresos, nueva línea de negocios o algún aspecto en particular que tenga relación con los accionistas de la compañía. Además, algo que tiene que aparecer indiscutiblemente es la seguridad, ir de la mano con ella, analizar todos los aspectos en los dispositivos y demás, en aras de la protección. Así mismo, las actualizaciones también se deben contemplar y las últimas tendencias sobre cómo se desarrolla el software con DevOps. Cuando se implementan soluciones de IoT, lo típico no es que esté en las mismas condiciones por mucho tiempo; son necesarias constantes actualizaciones para explotar mejor los datos. Es aconsejable mantener un continuo desarrollo con la seguridad adecuada, especialmente en servicios en la nube. Esto mismo debe suceder en *Edge* para cuando el cambio sea necesario.

Juan Francisco Jurado P.
Es un reto para las empresas introducir la computación *Edge* o *Fog*, dentro de la cultura de la organi-

zación, en la mentalidad de los usuarios. Una compañía que viva con la postura de hace 20 años, quebrará en los próximos dos. Eso implica cómo se maneja la información para asumir nuevas tecnologías. Solamente en el día a día mostrarán la necesidad de migración e implementación de nuevas tecnologías. Solo con esa mentalidad ambiciosa de generar impacto será posible. Técnicamente hablando con relación a la infraestructura y la ciberseguridad tienen que implementarlas y contemplar también un tema regulatorio. Una empresa, no necesariamente las grandes de Wall Street, deben estar muy relacionadas con la regulación para no verse inmiscuidas en vacíos legales, porque son nuevas y necesitan seguir ciertos patrones. Con relación a los aspectos en los que no se pueden equivocar las compañías, es sobre la visión de negocio. En mi corta experiencia de *startup* en *Sillicon Valley*, las empresas pueden verse como un millón de renacuajos que la mayoría muere. Bajo esa premisa no pueden permitir que el ecosistema los arrase, de cara al negocio. Es necesario considerar cómo generar valor que impacte a mi mercado, ligado a la mentalidad de cambio en los líderes de las empresas.

Jeimy J. Cano M.

Los invito a hacer sus recomendaciones finales, tanto para los desarrolladores como para las empresas que desean avanzar en estos nuevos escenarios de *Edge* y *Fog Computing.*

Juan Francisco Jurado P.

Invito a los desarrolladores y motivadores de que la 'magia negra'

exista a involucrarse en el concepto de que la tecnología cambia día a día y que no deben parar de aprender. Así mismo, a asumir los retos para el aprendizaje de cualquier tipo de tecnología. Sin duda, *Edge Computing* y *Fog Computing* están presentes en la cotidianidad. El mundo de este año 2020, no solo es importante por la pandemia o por las dificultades políticas y sociales que se registran en el mundo, está presente la necesidad de pensar para replantear las interacciones entre las personas, el monitoreo de todas las actividades de los usuarios. Recomiendo también tener en cuenta la importancia de estos nuevos desarrollos para formar parte de esa inmersión tecnológica que el mundo proporciona, tanto como Internet, IoT o inteligencia artificial, algunas veces inexplicables.

Julián Suárez R.

Invito a los desarrolladores y a las empresas a que se introduzcan en estas tecnologías de IoT, *Edge* y *Fog Computing*, desde la perspectiva de los beneficios para los nuevos negocios. La pandemia es una oportunidad para revisar los servicios y su evolución, hecho que los habilita. Les recomiendo contemplar la seguridad y los nuevos mecanismos de telecomunicaciones. Así mismo, continuar en ese camino de aprendizaje permanente para asumir los desarrollos actuales y los que vienen.

Felipe Nicolás Diniello

Hay un mundo por descubrir. Seguirán existiendo nuevas oportunidades de negocio, la realidad es que las bases están sentadas para la mayoría de las soluciones y en lo tecnológico para el desarrollo de cualquier cosa. Las posibilidades son inmensas, desde buscar nuevas soluciones; la seguridad es un tema crítico por explorar. Para los desarrolladores recomiendo aprender lo que está sobre la mesa para asumir el riesgo y detectar las manchas que puedan llegar al ecosistema.

***Sara Gallardo M**. Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; es editora de esta revista.*

Arquitectura resiliente empresarial

DOI: 10.29236/sistemas.n156a6

Una visión corporativa y prospectiva al 2025.

Resumen
Comprender la evolución acelerada de las organizaciones en el contexto de un escenario digital, significa actualizar las reflexiones empresariales respecto de las promesas de valor y los retos que imponen las nuevas expectativas de los clientes y las tecnologías emergentes. En este sentido, más allá de la continuidad del negocio, es necesario desarrollar una arquitectura resiliente empresarial que les permita tomar mayores riesgos, de manera de incorporar capacidades clave para proteger el modelo de generación de valor en escenarios cada vez más inestables y volátiles. Por lo tanto, este documento desarrolla una mirada prospectiva con distintos futuros posibles para esta arquitectura, con el fin de que las compañías cuenten con un referente base para tomar las decisiones requeridas, de cara al reto de la transformación digital que ellas enfrentan en la actualidad.

Palabras clave
Resiliencia, arquitectura, prospectiva, ciberseguridad, transformación digital

Introducción

El avance acelerado de la cuarta revolución industrial y la convergencia tecnológica entre lo físico, lo lógico y lo biológico establecen un nuevo escenario de reflexión y de negocios, que demanda una lectura enriquecida de la realidad. Esta nueva realidad establece un conjunto de exigencias y retos que están más allá de las prácticas de gobierno de tecnología de información y comunicaciones actuales, las cuales ahora deben ser leídas y reinterpretadas en un escenario ciberfísico, donde existe un aumento creciente de densidad digital, flujos de información conocidos y emergentes, y una mayor conectividad en diferentes contextos (Fatima, Anjum, Malik & Ahmad, 2020).

El entorno ciberfísico plantea una ruta diferente de comprensión de los retos empresariales, comoquiera que las organizaciones, no solo deberán estar atentas a que los clientes puedan concretar experiencias novedosas y agilizar sus actividades, sino que cualquier falla en este entorno puede llegar a afectar la integridad de la persona o brindarle información inexacta que la lleve a tomar decisiones inadecuadas. En este sentido, las condiciones de seguridad y control en lo ciberfísico se mueven entre los principios básicos de confidencialidad, integridad y disponibilidad, pasando por el "*safety*" (propio de la disciplina operativa en ambientes industriales) hasta llegar a la confiabilidad del dispositivo (Avizienis, Laprie, Randell & Landwehr, 2004).

En consecuencia, los entornos ciberfísicos demandan un panorama de seguridad y control con una vista de resiliencia y confiabilidad donde la gestión de riesgos tradicional basado en "cero riesgo" y "seguridad cien por ciento", se transforma en una lectura de umbrales de operación (IIA, s.f.) donde, tanto el proveedor del producto o servicio como los clientes, están involucrados todo el tiempo para hacer realidad la expectativa del usuario en esa experiencia emergente fruto de la convergencia tecnológica.

Así las cosas, es necesario plantear una vista prospectiva que permita tanto a las organizaciones como a sus proveedores, establecer patrones de transformación de mediano y largo plazo, con el fin de consolidar una ruta de resiliencia y confiabilidad basada en al menos cuatro estrategias clave: anticipación, prevención, detección y tolerancia (Saydjari, 2018), las cuales sirvan como marco de observación y reflexión para avanzar hacia el reconocimiento y puesta en operación de una nueva cultura organizacional, ya no sólo basada en proteger, sino en defensa, anticipación y fiabilidad.

Por tanto, este documento plantea y desarrolla un escenario prospectivo para una arquitectura resiliente empresarial, que permita a las empresas visualizar un posible camino de evolución para ajustarse a los retos que le plantea la cuarta revolución industrial, y así preparar la dinámica corporativa y la cultura organizacional para romper con la inercia que se trae de los marcos conocidos y prácticas estándares, con el fin de alinear la corporación con los desafíos que impone un contexto digital acelerado, con ecosistemas digitales, distintos actores, adversarios desconocidos y exigencias que aún no llegan (Ponemon, 2020).

Marco general de la prospectiva

Al desarrollar un ejercicio de prospectiva no se busca "predecir" el futuro, sino establecer posibles futuros alternativos para visualizar y desarrollar.

Es una manera de explorar y analizar las tendencias y señales emergentes que se advierten en el entorno y con ello trazar un mapa sobre un territorio inexplorado para identificar caminos que lleven a la organización a lograr una posición estratégica anticipada desde la ventana de tiempo actual (Hines & Bishop, 2015).

Los retos prospectivos implican la revisión y análisis de diferentes tendencias políticas, económicas, sociales, tecnológicas, legales y ambientales, con lo cual no es una tarea fácil establecer el marco de trabajo base para construir la propuesta de visión de futuro. Para el desarrollo del ejercicio, el contexto es fundamental por lo que muchos detalles deben ser consolidados y simplificados para darle forma a lo que podría ser las señales más relevantes que permitan delinear algo de lo que puede ocurrir en el mediano y largo plazo (Weick & Sutcliffe, 2007).

La prospectiva es una práctica de anticipación encaminada a crear mapas de ruta para que las empresas cuenten con orientación sobre aspectos específicos de su interés, basada en información confiable, cierta y veraz, y al mismo tiempo en apuestas especulativas y exploratorias que científicos o tanques de pensamiento pueden hacer respecto de los temas de interés de la organización.

Cuando se desarrolla una prospectiva no se buscan certezas, sino respuestas parciales e incompletas, que la organización en el desarrollo mismo de sus actividades, le da forma para ir visualizando aquello que se establece en el mapa de ruta. No es un objetivo que permanece inmóvil todo el tiempo, sino que puede tener cambios por las inestabilidades que afectan el contexto.

Dichos cambios tendrán mayor o menor impacto dependiendo de nivel de la inestabilidad o volatilidad de la tendencia que se identifique

en el sector particular de negocio o a nivel global (Popper, 2008; Menon & Kyung, 2020).

Particularmente el resultado de los análisis desarrollados alrededor de la arquitectura resiliente empresarial, busca coordinar y orquestar diferentes tendencias y retos que se tienen en la actualidad desde la seguridad de la información, la ciberseguridad, la privacidad, la resiliencia, la confiabilidad y la operación de las infraestructuras, con el fin de delinear una vista enriquecida del nuevo estándar de gestión que las empresas deben asumir, para desinstalarse de las certezas y respuestas conocidas del entorno.

Los resultados que se presentan a continuación fruto de la revisión de patrones emergentes y señales débiles del ambiente, que se han identificado luego de la inmersión y correlación de diferentes documentos, reportes y artículos en las temáticas previamente mencionadas para darle forma a la visualización de la arquitectura resiliente empresarial, plantea una visión de evolución futura que permite a las organizaciones advertir los retos, riesgos y oportunidades que deben apropiar al transformar la gestión de riesgos en una práctica de umbrales, tolerancia y pronóstico distinta a la lectura vigente basada en certezas y análisis causa-raíz.

Arquitectura resiliente empresarial, una revisión conceptual

Una arquitectura resiliente empresarial no es un concepto que habla de invulnerabilidad, sino de la capacidad que tiene una organización de evolucionar y adaptarse en escenarios volátiles, inciertos, complejos y ambiguos, expuesta a amenazas y riesgos emergentes con adversarios conocidos y desconocidos, para lo cual diseña, configura y armoniza cuatro estrategias básicas: anticipación, prevención, detección y tolerancia, que definen la manera como la organización navega, entiende y da respuesta a los cambios e inestabilidades de su entorno (Saydjari, 2018).

Esta capacidad demanda desinstalarse de las certezas, asumir aquello que no sale como estaba previsto como una oportunidad de aprendizaje y explorar todo el tiempo el contexto para comprender qué es lo que hace fallar las medidas de control, y no buscar culpables en las personas, dado que la inevitabilidad de la falla es aquello que es esperado en ellas (Woods, Dekker, Cook, Johannesen & Sarter, 2010).

De esta forma, se advierte una lectura de la dinámica de la operación como un ejercicio de umbrales, que inicia con el apetito al riesgo que la compañía declara frente a su estrategia, que luego se enmarca en un nivel de tolerancia, donde la organización se mueve de forma cómoda frente al escenario adverso y que termina en una capacidad de

riesgo que declara el máximo nivel exposición que la organización puede soportar (IIA, s.f.; GAO, 2016).

La estrategia de anticipación busca establecer oportunidades y ventanas de acción previas para manejar las situaciones adversas y definir marcos de actuación concretos que habiliten a la organización avanzar en medio del evento incierto, en ese momento no conocida para el entorno, pero visualizada y analizada por adelantado en la empresa, con el mínimo de inciertos y consecuencias. La estrategia de anticipación nuevamente no es una predicción, sino un pronóstico, una lectura en contexto de las tendencias e información disponibles para avanzar donde otros no saben cómo hacerlo.

La estrategia de prevención está situada en la zona de los datos y la revelación de situaciones potencialmente agresivas contra la esencia de los objetivos empresariales. Esta estrategia se funda en propuestas basadas en analítica de datos, valoración y análisis de riesgos conocidos y latentes (Cano, 2017), identificación de patrones y prácticas concretas en las personas que movilizan esfuerzos en aquellas zonas grises que la organización tiene.

La estrategia de detección es la manera tradicional como la organización identifica que alguna situación particular no concuerda con los estándares normales. Esto se traduce en la activación de las alertas y mecanismos de bloqueo de la situación que genera la amenaza.

La detección será más efectiva mientras se cuente con mayor conocimiento del riesgo o amenaza y podrá afinarse su efectividad, en la medida que se tenga mayor información y se ajuste su operación.

La estrategia de tolerancia es la definición de los umbrales de operación permitidos frente al evento incierto. Son todos aquellos mecanismos que brindan tiempo extra a la empresa en medio de la adversidad y que no podrá sobrepasar la capacidad de riesgo definido por la organización.

Arquitectura Resiliente Empresarial. Prospectiva al 2025

Considerando los elementos conceptuales establecidos en la sección anterior, se presenta a continuación la visión prospectiva de la arquitectura resiliente empresarial al 2025, que se explicará en la Figura 1.

La prospectiva realizada se basa en la transformación digital que las empresas están desarrollando y que terminará cambiando la manera como hacen las cosas en un entorno hiperconectado, hiperautomatizado e hiperaumentado, en el cual las amenazas y tensiones emergentes mutarán y por tanto, habrá menos certezas para abor-

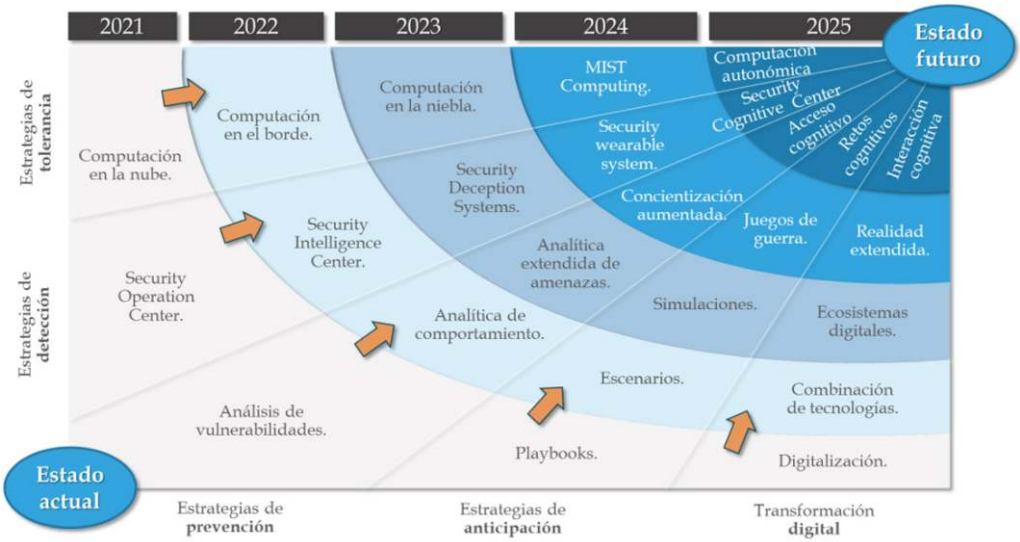


Figura 1 Arquitectura Resiliente Empresarial - Prospectiva 2025 (Elaboración propia)

dar situaciones cada vez más inesperadas (Valdez-de-León, 2019).

La presentación de la prospectiva por las estrategias definidas es acumulativa, es decir cumplir con lo establecido para un año, significa incorporarlo en el año siguiente y avanzar con la puesta en operación de la siguiente propuesta detallada. Así para la estrategia de anticipación, se inicia con los *playbooks* en el 2021 y en el 2022, la idea es madurar en la práctica anterior y evolucionar hacia los escenarios.

Estrategia de anticipación

La evolución que se plantea para las estrategias de anticipación se basa en la reducción de incierto en las actuaciones de las empresas. Los *playbooks* se configuran como los libros de trabajo permanentes donde las organizaciones se preparan para actuar frente a eventos conocidos (o semejantes) con el fin de establecer el marco de acción requerido para minimizar los posibles impactos del incidente que se tiene en la empresa, de esta forma asegura un adecuado tratamiento del evento y el marco de debido cuidado requerido frente a sus grupos de interés (Kick, 2014).

Los escenarios se plantean como el siguiente paso en esta estrategia. Los escenarios son ejercicios de construcción colectiva, basados en reflexión y análisis, que buscan establecer situaciones posibles y probables para las organizaciones con el fin de indagar en las tendencias y retos emergentes de la empresa y cómo ésta debe maniobrar en el momento que corresponda (Hines & Bishop, 2015). El caso más relevante de aplicación de es-

te ejercicio son los logros de equipo ejecutivo de Shell Corp. en la década de los sesenta cuando plantearon el escenario de la caída de precios del petróleo en 1973 y detallaron las diferentes acciones para sortear este momento, lo que les permitió actuar con claridad en medio de las inestabilidades de aquella situación.

Madurar en la práctica de *escenarios* establece la transformación de la empresa y su equipo ejecutivo para avanzar en el incierto. De igual forma, el siguiente paso propuesto es irrumpir en un mayor apetito al riesgo que necesariamente implica moverse al dominio de las simulaciones, donde lo importante es observar y determinar los comportamientos, riesgos, retos y resultados de las propuestas novedosas para la organización (Popper, 2008). Es importante aclarar, que no se tendrán todas las respuestas, sino el marco general de comprensión de lo que puede ser y los posibles impactos que se pueden presentar.

Luego de las *simulaciones*, que buscan no solamente enfrentarse al incierto, sino comprender la complejidad de las situaciones que se ven hacia adelante, se llama a una incorporación de un ejercicio denominado juegos de guerra. Los juegos de guerra son juegos de estrategia propios del entorno militar, donde se reconocen actores particulares, con capacidades específicas para movilizar acciones que puedan afectar a su contraparte (Alkire, Lingel & Hanser, 2018). En el entorno empresarial, implica conocer la dinámica de los negocios y los diferentes participantes de su sector, para que la empresa se mantenga en modo "radar" es decir, explorando e identificando aspectos de su entorno digital para capitalizar como oportunidad o reconociendo posibles amenazas para actuar de manera anticipada y aumentar su capacidad de respuesta ágil y efectiva.

El siguiente nivel en la evolución planteada para esta estrategia se funda en los recientes avances del uso de algoritmos de aprendizaje (supervisados y no supervisados) los cuales son capaces de plantear retos cognitivos, que configuran combinaciones de escenarios y situaciones basados en lógicas conocidas y aleatorias, creando contexto inciertos e inesperados para tratar de advertir situaciones que aún no se desarrollan o insinúan en las mejores estimaciones (Cano, 2020). Este tipo de rutinas de prospectiva cognitiva, asistida por algoritmos debe pasar primero por ejercicios de simulación para establecer sus posibilidades y limitaciones, y así establecer sus posibles usos y capacidades de cara a los desafíos que enfrentarán las organizaciones en la industria 4.0 y su transición hacia la sociedad 5.0

Estrategia de prevención

La prospectiva planteada en esta estrategia busca identificar en marcos de tiempo cortos aquellas si-

tuaciones que pueden desestabilizar rápidamente la organización y afectar sus operaciones. En este sentido, los temas de seguridad y control advierten momentos que pueden llegar a afectar los planes de las empresas y generar controversias que terminen afectando la estrategia de la compañía.

El *análisis de vulnerabilidades* como práctica conocida en seguridad, es un ejercicio de cierre de brechas identificadas. Las herramientas disponibles sobre este tema cuentan bien con firmas de ataques o algunas heurísticas que pueden generar condiciones de error o falla que implique revisar en detalle tanto el software como el hardware. Una práctica madura de análisis de vulnerabilidades debe estar asistida por la gestión de las fallas identificadas y el aseguramiento de los parches que se necesitan para cerrar las limitaciones que se advierten (Pillay, 2019).

Un segundo momento de la evolución es avanzar con la *analítica de comportamiento*. Este paso supone contar con sensores y formas de recoger las actuaciones de las personas, procesos o aplicaciones en la organización, de tal forma que se puedan establecer patrones de comportamiento concretos y advertir desviaciones sobre lo que inicialmente puede estar ocurriendo (Addae, Sun, Towey et al., 2019). Es importante advertir que los comportamientos pueden ser de diferente índole, desde la cadencia para escribir en el teclado, dinámica de acceso a las aplicaciones, archivos más consultados, aplicaciones más utilizadas, tráfico menos común o tendencias en utilización de procesamiento o almacenamiento en disco. La analítica de comportamiento genera alertas para atender y actuar en consecuencia.

La *analítica extendida de amenazas* es un momento de quiebre en la estrategia de prevención. Esta tendencia introduce la convergencia entre la inteligencia de amenazas y las amenazas inteligentes. Mientras la inteligencia de amenazas evalúa, integra, analiza e interpreta los datos que ha reunido, para establecer un panorama concreto al que puede enfrentarse la organización en corto y mediano plazo, las amenazas inteligentes establecen el uso adversarial de la inteligencia artificial para retar los mecanismos de seguridad y control disponibles, con el fin de crear entornos de ataque por fuera de los análisis de los datos disponibles o posiblemente alterados por algoritmos diseñados para tal fin (Yampolskiy, 2017).

La *concientización aumentada* se traduce en el uso de las experiencias del mundo aumentado por la realidad virtual, la realidad aumentada y la realidad mixta, para conectar mejor la experiencia de una persona frente al ejercicio de protección y aseguramiento de la información. Esta nueva propuesta puede bien sumergir al individuo en un

escenario completamente virtual donde puede interactuar, ver objetos simulados y los efectos de sus actuaciones, o tomar la realidad y complementarla con objetos virtualizados creando una sensación de inmersión en un escenario real donde puede ver los efectos de sus acciones, o unir los dos conceptos anteriores para facilitar una experiencia aumentada según la necesidad que se plantee por la organización (Carmigniani, Furht, Anisetti et al., 2011).

El *acceso cognitivo* es una nueva frontera donde en un contexto asistido por ecosistemas digitales, geolocalización y controles de acceso basados en biometría avanzada, una persona puede ser reconocida por un algoritmo y establecer de forma automática el perfil de acceso que requiere, cruzando los datos disponibles a la fecha. Este tipo de algoritmos de aprendizaje, por lo general supervisados, debe cuidar su fase de entrenamiento para configurar adecuadamente la estrategia de acceso bien a instalaciones físicas, aplicaciones o infraestructuras tecnológicas. La dependencia y retos que implica basar el control de acceso a este tipo de tecnologías deberán primero pasar por los ejercicios de simulación para detallar mejor las implicaciones positivas, así como sus limitaciones y retos.

Estrategia de detección

La detección supone contar con información suficiente para analizar y establecer patrones de acción que permitan levantar alertas, bien basados en firmas de ataques o vulnerabilidades conocidas, lo que actualmente desarrolla un SOC (*Security Operation Center*). Este tipo de servicios observan en tiempo real eventos, identifican desviaciones sobre patrones conocidos, que permiten reaccionar una vez confirmada la anomalía siguiendo un conjunto de reglas previamiente definidas (Jacobs, Arnab & Irwin, 2013).

La evolución de este tipo de servicios se mueve al SIC (*Security Intelligence Center*) donde se adelanta identificación de patrones emergentes, analítica de eventos inusuales en tiempo real, con una perspectiva más proactiva y basado en heurísticas. Esta nueva posibilidad permite a las organizaciones avanzar en una detección anticipada de posibles amenazas y desarrollar una capacidad de acción preventiva más eficiente y concreta de cara a los retos de nuevos productos y servicios que la organización desea desplegar en el contexto digital.

Los sistemas de engaño (*Deception Systems*) tienen como propósito crear un escenario de mayor incierto para el adversario, una estrategia que busca recrear un entorno simulado muy cercano a la realidad y sus condiciones, para que el atacante trate de ingresar y desde allí estudiar con detenimiento sus movimientos y estrate-

gias. Las tecnologías de engaño requieren un nivel de madurez y desarrollo de la infraestructura tecnológica, así como una gestión de seguridad y ciberseguridad basada en una postura defensiva, la cual se traduce en demorar al atacante antes de que tenga éxito (Wang & Lu, 2018).

La detección deberá migrar para incorporarse no solamente a la infraestructura corporativa sino al mundo físico de la ropa inteligente u objetos vestibles, con tecnologías de seguridad para vestibles (*security wearable systems*). El aumento de la densidad digital para transformar el mundo tangible y visible, establece un referente de transformación digital que buscan agregar nuevas funcionalidades a diferentes objetos del mundo real para crear condiciones aumentadas y con inteligencia que hagan más atractivos estos objetos. Camisetas, gafas, relojes, pañales, chaquetas autoajustables, zapatos deportivos, entre otros, con inteligencia artificial incorporada, establece una nueva frontera en la detección y alerta de seguridad y control. El mundo estará ahora con efectos concretos y reales de las posibles fallas del software o el hardware de forma más evidente.

En la frontera de la evolución se introduce el concepto de SCC (*Security Cognitive Center*), que ya no sólo incorpora los retos propios del SOC y del SIC, sino de los nuevos objetos vestibles, para desarrollar escenarios emergentes, ejecutar simulaciones de ataques inusuales, aprender de la dinámica del entorno y configurar pronósticos de amenazas, donde los algoritmos de inteligencia artificial son los protagonistas.

Este nuevo concepto implica reconocer las tasas de error de los algoritmos que se implementen, así como el desarrollo de una contrainteligencia cognitiva que permita validar que los programas diseñados se ajustan a los diseños establecidos y sus estrategias de aprendizaje se mantienen dentro de los parámetros programados.

Estrategia de tolerancia

La tolerancia implica poder tener opciones para responder en medio de tensiones y acciones agresivas sobre la infraestructura o procesos de la empresa. Esto es, mecanismos diseñados para recuperar y restaurar las funcionalidades críticas luego de un ataque exitoso (Jackson, 2009). En este contexto, *la computación en la nube* se ha convertido en un elemento base de las empresas del siglo XXI donde se toma una decisión informada para trasladar las capacidades de procesamiento y almacenamiento a un tercero, que generalmente con bajo costo, mantiene y asegura la información de las empresas basado en un esquema de contratación elástico que se traduce en “cobro por uso” y manejo de umbrales disponibles y acordados (Velte, Velte & Elsenpeter, 2010).

Si bien la computación en la nube se ha consolidado como un marco de trabajo base para las empresas, empieza un nuevo avance hacia la *computación en el borde*. Esta nueva computación que se incorpora por el aumento de dispositivos inteligentes conectados y enlazados con aplicaciones en la nube, los cuales serán accedidos desde dispositivos móviles (Zalewski, 2019). La *computación en el borde* no son nuevos dispositivos, es una decisión de arquitectura que busca disminuir la latencia de conexión y aumentar la capacidad de procesamiento para lograr la experiencia requerida al interactuar con un objeto con mayor densidad digital. Esta nueva apuesta, más allá de la nube, establece una vista de confiabilidad que demanda un alto nivel de tolerancia para asegurar que los datos estén más cerca de los usuarios y permitir una mayor velocidad de las aplicaciones (Overby, 2020).

La *computación en la niebla* es un concepto de una estructura de red que se extiende desde los bordes exteriores de la organización donde se crean los datos hasta dónde se almacenarán, ya sea en la nube o en el centro de datos de un cliente. Es una capa de conectividad extendida que permite acelerar la conexión con baja latencia, para luego conectarse con el sitio en la nube donde están los datos. En general se establecen diferentes nodos interconectados que mantienen la conectividad, con el fin de disminuir el ancho de banda requerido y así acelerar la respuesta de las aplicaciones para lograr una experiencia en tiempo real. Este paradigma de computación, advierte retos de seguridad y control que deberán asegurarse de cara a su incorporación y soporte en el futuro (Yahuza et al., 2020; Tozzi, 2020).

La *computación por bruma* (*MIST Computing*) es el siguiente paradigma que la organización deberá entender, comprender e incorporar. Esta computación es el extremo de una red, típicamente compuesta de microcontroladores y sensores. Utiliza microcomputadoras y microcontroladores para alimentar los nodos de computación de la niebla y potencialmente seguir adelante hacia los servicios de computación centralizados (en la nube). Dos objetivos clave de la computación por bruma son:

- Permitir la recolección de recursos mediante capacidades de computación y comunicación disponibles en el propio sensor.
- Permitir que los cálculos arbitrarios sean aprovisionados, desplegados, administrados y monitoreados en el propio sensor (Radiocrafts, 2019).

En pocas palabras, la computación por bruma está cerca de los dispositivos inteligentes de los usuarios para procesar sus flujos de información, desarrollar analítica de datos y habilitar mecanismos que aseguren su privacidad.

Finalmente, se advierte el desarrollo de una propuesta de computación que en su diseño y configuración implica materializar la resiliencia computacional de una máquina. La *computación autónoma* (o autonómica) propuesta por Paul Horn de IBM en 2001, se refiere a las características de autogestión de los recursos informáticos distribuidos, que reconocen y comprenden los cambios en el sistema, con el fin de tomar las medidas correctivas apropiadas de forma automática, con mínima intervención humana. Las características de este tipo de computación según IBM son: (Gibbs, 2002)

- Poseen un sentido de sí mismos.
- Se adaptan a los cambios en su entorno.
- Se esfuerza por mejorar su rendimiento.
- Se reparan cuando advierten un daño.
- Se defienden contra adversarios.
- Intercambia recursos con sistemas poco familiares.
- Se comunica a través de estándares abiertos.
- Anticipan las acciones de los usuarios.

Lograr configurar una computación autónoma implica reconocer inteligencia avanzada en las máquinas, que les permite mantener un nivel de monitorización y pronóstico automatizado que limita y anticipa el deterioro del mismo sistema, de tal manera que la intervención humana se limita a actividades de mantenimiento de la infraestructura en sí misma, dejando la evolución y aseguramiento del sistema a la lógica y capacidad resiliente inherente al diseño del sistema mismo.

Esta vista evolutiva de la tolerancia incorpora capacidades inteligentes tanto en la infraestructura como en el software de las máquinas para mantener la conectividad, el procesamiento y las aplicaciones en condiciones óptimas de uso y despliegue, facilitando su escalamiento y aseguramiento en mediano y largo plazo.

Si bien, muchas de estas promesas están en desarrollo y ya se cuentan con avances sustanciales, las organizaciones deberán ejecutar prototipos para aprender de las dinámicas de estos nuevos paradigmas de la computación que pronto estarán disponibles y abiertos para las empresas que se muevan hacia entornos más digitales y tecnológicamente modificados.

Reflexiones finales

Entender los nuevos entornos de negocios mediados por contextos tecnológicamente modificados y con ecosistemas digitales, es comprender que las promesas de valor se transforman y cambian de manera acelerada por las exigencias de experiencias distintas por parte de los clientes. En consecuencia, las organizaciones deberán tomar cada vez más riesgos para asegurar las capacidades requeridas que

den cuenta con los retos que implica ser cada día más digital y menos análogo (Stafford & Schindlinger, 2019).

En este escenario, las empresas estarán más interconectadas y visibles al mundo, lo cual implica mayores oportunidades para ser parte de apuestas de productos y servicios novedosos, así como parte de proyectos conjuntos que buscan crear espacios de co-creación claves para lograr innovaciones que cambien la manera de hacer las cosas. Así las cosas, la colaboración y conexión entre las diferentes organizaciones participantes, hará que se requiera un acoplamiento e interacción entre las infraestructuras, aplicaciones y datos para concretar los nuevos desarrollos esperados (Fatima, Anjum, Malik & Ahmad, 2020).

Por lo tanto, habrá una mayor exposición de las compañías y por ende un espacio de acción para actividades no autorizadas y la aparición de adversarios, que pueden capitalizar las limitaciones y riesgos propios de esta mayor conectividad, interacción y acoplamiento (Denyer, 2017). Cuanto mayor sea la apertura e interacción, el uso de tecnología abiertas y en manos de terceros, menos control se tendrá sobre el aseguramiento de las mismas y por tanto, la capacidad de respuesta ante eventos inesperados deberá ser la norma que guíe la relación con sus terceros de confianza.

La arquitectura resiliente organizacional deberá ser una norma base de las empresas en los próximos diez años, comoquiera que no hacerlo, la expone a un amplio abanico de posibilidades actuales y futuras, que pueden ser aprovechadas por agentes agresores, para impedir la exploración de oportunidades de negocio, creando un impuesto digital al desarrollo empresarial que se verá materializado en la explotación de vulnerabilidades y brechas que deteriorarán la reputación corporativa, marginando a la compañía de nuevos negocios o apuestas innovadoras (Dupont, 2019).

Contar con una arquitectura resiliente empresarial es apostarle a la viabilidad de la empresa en el contexto digital, es construir una red de protección y aseguramiento con los terceros de confianza y reconocer que, a pesar de las condiciones de operación y acuerdos clave efectuados con los proveedores, la inevitabilidad de la falla estará presente y tendrá que atender los incidentes que se manifiesten, para lo cual la mencionada arquitectura deberá dar los lineamientos y posibilidades claras para responder con claridad en medio de la incertidumbre y la inestabilidad que pueda ocasionar un evento inesperado.

La prospectiva planteada en este documento es una visión de posibles futuros que las organizaciones pueden revisar para avanzar hacia una sociedad cada vez más digital,

con distintos actores y nuevas demandas sociales, de manera que cada empresa revise las diferentes rutas y tome las decisiones que sean del caso, teniendo en cuenta cómo evoluciona su apetito al riesgo en medio de un aumento exponencial de la densidad digital en su entorno de negocio.

Referencias

Addae, J.H., Sun, X., Towey, D. et al. (2019) Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter*. 29. 701–750. Doi: 10.1007/s11257-019-09236-5

Alkire, B., Lingel, S. & Hanser, L. (2018). A Wargame Method for Assessing Risk and Resilience of Military Command-and-Control Organizations. *Rand Corporation*. Doi: 10.7249/TL291

Avizienis, A., Laprie, J., Randell, B. & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*. 1(1). 11-33. Doi: 10.1109/TDSC.2004.2

Cano, J. (2017). The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security. *ISACA Journal*. 5.

Cano, J. (2020). Retos de seguridad/ciberseguridad en el 2030. Reflexión sobre un ejercicio prospectivo incompleto. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 154. 68-79. Doi: 10.29236/sistemas.n154a7

Carmigniani, J., Furht, B., Anisetti, M. et al. (2011) Augmented reality technologies, systems and applications. *Multimed Tools Appl*. 51, 341–377. Doi: https:10.1007/s11042-010-0660-6

Denyer, D. (2017). Organizational resilience. A summary of academic evidence, business insights and new thinking. *BSI-Crandfield University*. De: https://www.cranfield.ac.uk/som/case-studies/organizational-resilience-a-summary-of-academic-evidence-business-insights-and-new-thinking

Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience. *Global Risk Institute*. De: https://globalriskinstitute.org/publications/the-cyber-resilience-of-financial-institutions-a-preliminary-working-paper-on-significance-and-applicability-of-digital-resilience/

Fatima, I., Anjum, A., Malik, S. & Ahmad, N. (2020) Cyber Physical Systems and IoT: Architectural Practices, Interoperability, and Transformation. *IEEE IT Professional*. May/June. 46-54. Doi: 10.1109/MITP.2019.2912604

GAO (2016). Enterprise risk management. Selected Agencies' Experiences Illustrate Good Practices in Managing Risk. De: https://www.gao.gov/assets/690/681342.pdf

Gibbs, W. (2002) Autonomic computing. *Scientific American*. De: https://www.scientificamerican.com/article/autonomic-computing/

Hines, A. & Bishop, P. (2015). *Thinking about the future: Guideline for strategic foresight*. Second Edition. Houston, TX. USA: Hinesight.

IIA (s.f.). Definición e implantación de apetito al riesgo. Fábrica de Pensamiento. *Instituto de Auditores Internos de España*. De: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf

Jackson, S. (2009). *Architecting resilient systems. Accident Avoidance and Survival and Recovery from Disruptions*. Hoboken, NJ. USA: John Wiley & Son

Jacobs, P., Arnab, A. & Irwin, B. (2013) Classification of Security Operation Centers. *2013 Information Security for South Africa*, Johannesburg. 1-7, Doi: 10.1109/ISSA.2013.6641054.

Kick, J. (2014). Cyber Exercise Playbook. *MITRE Report*. De: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Menon, G. & Kyung, E. (2020). When More Information Leads to More Uncertainty. *Harvard Business Review*. De: https://hbr.org/2020/06/when-more-information-leads-to-more-uncertainty

Overby, S. (2020). Edge computing for beginners: 11 key concepts. *Enterprisers Project*. De: https://enterprisersproject.com/article/2020/7/edge-computing-beginners-11-concepts

Pillay, R. (2019). *Learn penetration testing. Understand the art of penetration testing and develop your white hat hacker skills*. Birmingham, UK.:Packt Publishing Ltd

Ponemon (2020). Digital transformation & cyber risk. What do you need to know to stay safe. *CyberGRX*. De: https://get.cybergrx.com/ponemon-report-digital-transformation-2020

Popper, R. (2008). How are foresight methods selected? *Foresight*. 10(6). 62-89. Doi: 10.1108/14636680810918586

Radiocrafts (2019) Cloud vs Fog vs Mist Computing, Which One Should You Use? De: https://radiocrafts.com/cloud-vs-fog-vs-mist-computing-which-one-should-you-use/

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Stafford, B. & Schindlinger, D. (2019). *Governance in the digital age. A guide for the modern corporate board director*. Hoboken, N.J. USA: John Wiley & Sons

Tozzi, C. (2020). The pros and cons of adding edge computing to a cloud architecture. *TargetTec*h. De: https://searchcloudcomputing.techtarget.com/tip/The-pros-and-cons-of-adding-edge-computing-to-a-cloud-architecture

Valdez-de-León, O. (2019). How to Develop a Digital Ecosystem: a Practical Framework. *Technology Innovation Management Review*. 9(8). 43-54. http://doi.org/10.22215/timreview/1260

Velte, A., Velte, T. & Elsenpeter, R. (2010). *Cloud computing. A practical approach*. New York, USA: McGraw Hill.

Wang, C. & Lu, Z. (2018). Cyber Deception: Overview and the Road Ahead. *IEEE Security & Privacy*. 16(2). 80-85. Doi: 10.1109/MSP.2018.1870866.

Weick, K. & Sutcliffe, K. (2007). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty*. Second Edition. San Francisco, CA. USA: Jossey-Bass

Woods, D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. (2010). *Behind human error*. Second Edition. Farnham, Surrey. England: Ashgate Publishing Limited.

Yahuza, M. et al. (2020). Systematic Review on Security and Privacy Require-

ments in Edge Computing: State of the Art and Future Research Opportunities. *IEEE Access*. 8. pp. 76541-76567. Doi: 10.1109/ACCESS.2020.2989456.

Yampolskiy, R. (2017). AI Is the Future of Cybersecurity, for Better and for Worse. *Harvard Business Review*. De: https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

Zalewski, J. (2019). IoT Safety: State of the art. *IEEE IT Professional*. 21(1). 16-20. Doi: 10.1109/MITP.2018.2883858

Jeimy J. Cano M., Ph.D, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Un acercamiento a *fog computing*

DOI: 10.29236/sistemas.n156a7

Conceptos claves, ventajas y principales desafíos

Resumen
Los sensores y otros dispositivos de Internet de las Cosas (IoT) generan voluminosos, variados y veloces datos primarios que pueden incluir ruido, irrelevancia y poca sensibilidad al contexto, además de crearse, con bastante frecuencia, con una alta distribución geográfica. La transferencia de tales datos directamente a la nube genera incremento de errores, pérdida de datos y alta probabilidad de congestión de tráfico en la red, además de un gasto considerable de recursos, sin una ganancia asociada. Con el fin de disminuir la latencia y el tráfico innecesario de datos en Internet, mediante el aprovechamiento de recursos distribuidos geográficamente más cerca de la fuente, surge el paradigma *Fog computing,* conformando un ecosistema *IoT-Fog-Cloud*. El presente artículo ofrece un acercamiento conceptual a *fog computing*, expone sus ventajas y los tipos de aplicaciones IoT para las cuales es más apropiado su uso. Finalmente, se resumen los desafíos más importantes asociados a tal enfoque emergente.

Palabras claves:
fog computing, IoT, *edge computing*, desafíos tecnológicos

Introducción

Mientras la computación en la nube ha sido una tecnología habilitadora clave para Internet de las Cosas (IoT), el crecimiento exponencial de los datos generados que ya alcanzan varias decenas de miles de millones de sensores y actuadores, está estresando las infraestructuras actuales basadas en la nube, al tratar de satisfacer los niveles tradicionales de calidad de servicios (QoS).

Para lidiar con esta problemática, surge un nuevo paradigma de computación que fuera acuñado por Cisco en 2012 como *fog computing* (Bonomi, Milito, Zhu, & Addepalli, 2012), computación en la niebla (en castellano). Con el fin de disminuir la latencia y el tráfico innecesario de datos en Internet, mediante el aprovechamiento de recursos distribuidos geográficamente más cerca de la fuente, este paradigma complementa a la computación en la nube, sirviendo de capa entre los dispositivos de IoT y la nube (Tárano, Delgado, & Pérez, 2018), (Buyya & Narayana-Srirama, 2019).

El presente artículo está encaminado a ofrecer un acercamiento conceptual a *fog computing*, exponer sus ventajas y los tipos de aplicaciones IoT para las cuales es más apropiado su uso. Finalmente, se resumen los desafíos más importantes asociados a tal enfoque emergente.

Breve bosquejo teórico sobre *fog computing*

Existe cierta confusión entre computación en el borde (*edge*), la niebla (*fog*), los llamados cloudlets, entre otros términos; todos ellos, derivados del paradigma computación en la nube (*cloud computing*).

Muy brevemente se explicarán a continuación algunos rasgos de las definiciones de varios de estos términos (Heck, Edinger, Schäfer, & Becker, 2018), con el empleo de la terminología original en inglés para evitar nuevas interpretaciones o ambigüedades en sus significados:

- *Cloudlets*: Son frecuentemente referidos como “centro de datos en una caja”. Constituyen por lo general computadoras potentes o clusters de computadoras que están bien conectados a Internet y localizados en una ubicación fija en el borde de la red. Exhiben ciertas limitaciones respecto a la niebla, por el hecho que son típicamente accedidos sobre Wi-Fi (aunque más recientemente se acceden sobre redes móviles) y no interactúan con la nube, meramente ofrecen recursos cercanos a los dispositivos IoT. En la actualidad se han extendido algunos marcos de arquitecturas de tres capas para los *cloudlets* que se interconectan con la nube, actuando como nodos niebla (*fog nodes*).

- *Fog computing*: Se define como una plataforma altamente virtualizada que provee computación, almacenamiento y servicios de red entre los dispositivos del usuario (IoT), al ubicarse cerca de ellos, y los centros de datos basados en computación en la nube. La arquitectura de tres capas de *fog computing* se abordará próximamente en la descripción de la arquitectura de referencia.

- *Edge computing*: A diferencia de la computación en la niebla, *edge computing* o computación en el borde se enfoca más en la cooperación entre dispositivos conectados de IoT, sin involucrar otros recursos de la red más poderosos, y no interactúan con la nube. Muchas veces se ubica su funcionalidad en los *gateways* que conectan los sensores y/o actuadores.

- *Mobile Edge Computing* (MEC): Limitado a las redes móviles, puede ser considerado un caso de *fog computing*, con interoperabilidad comprometida. Los servidores MEC proveen servicios de tecnología de información y servicios de virtualización típicamente dentro del radio de acceso de la red y en la proximidad cercana a dispositivos móviles y sensores conectados.

En la tabla 1 se resumen las características de cada uno de estos conceptos en el marco del paradigma *fog-edge computing*, atendiendo a la taxonomía de parámetros de desempeño propuesta por (Heck, Edinger, Schäfer, & Becker, 2018).

Tabla 1. Taxonomía de desempeño del paradigma *fog-edge computing*- adaptada de (Heck, Edinger, Schäfer, & Becker, 2018).

	MCC Cloudlets	***Fog Computing***	***Edge Computing***	***MEC Mobile Edge Computing***
fiabilidad	limitada	Sí	limitada	Sí
baja latencia	Sí	Sí	Sí	Sí
sensibilidad al contexto	limitada	Sí	Sí	Sí
geo-distribución	No	Sí	Sí	Sí
soporte movilidad	No	Sí	Sí	Sí
escalabilidad	No	Sí	limitada	Sí
interoperabilidad	No	Sí	Sí	limitada
eficiencia de energía	Sí	Sí	Sí	Sí
ahorro de ancho de banda	Sí	Sí	Sí	Sí

Se aprecia en la tabla 1 que todos los tipos de tecnologías del ecosistema *fog-edge* evaluadas cumplen los parámetros de baja latencia, eficiencia energética y ahorro de ancho de banda, que las distinguen de la computación en la nube; sin embargo, sólo el paradigma *fog computing* cumple plenamente todos los restantes parámetros de desempeño en su conjunto.

Más adelante se amplían las ventajas del mismo.

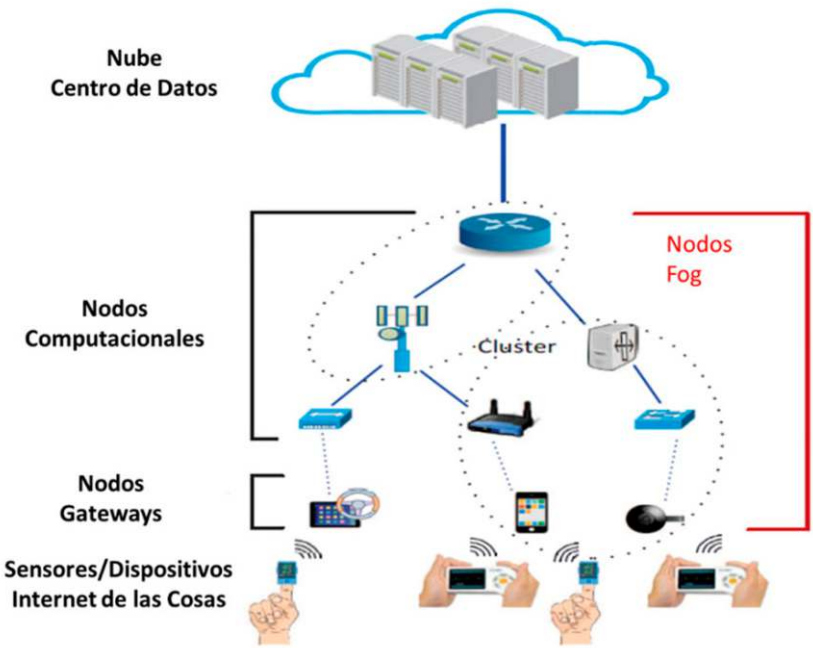
Arquitectura de referencia de *fog computing* - *OpenFog*

Las arquitecturas de la niebla mueven selectivamente la computación, el almacenamiento, la comunicación, el control y la toma de decisiones más cerca del borde de la red, donde los datos están siendo generados, con vistas a resolver las limitaciones de las actuales infraestructuras para habilitar casos de uso de densidad de datos y misiones críticas (IEEE Standards Association, 2018).

Según el Consorcio *OpenFog* los pilares claves de la arquitectura de *fog computing* son: (1) seguridad, (2) escalabilidad, (3) apertura, (4) autonomía, (5) fiabilidad, disponibilidad y capacidad de ofrecer servicios, (6) agilidad, (7) jerarquía, (8) capacidad de programación.

Los nodos de niebla se distribuyen en niveles jerárquicos, como se muestra en la figura 1. Un nodo *fog*

Figura 1: Ambiente general de computación en la niebla - adaptado de (Mahmud, Koch, & Buyya, 2018)



puede ser equipado con un núcleo de procesamiento, memoria, almacenamiento y ancho de banda (Mahmud, Koch, & Buyya, 2018).

Estos recursos pueden ser virtualizados y compartidos en la forma de micro instancias de computación (MCI). El nivel inferior de los nodos niebla reside muy cerca de los dispositivos IoT y usualmente ofrece interfaces de las aplicaciones asociadas. Todos los nodos niebla no están activos al mismo tiempo, lo que asegura un uso eficiente de la energía y un nivel de escalabilidad selectivo.

Ventajas del paradigma de computación en la niebla

El modelo *fog computing* consigue reducir el tráfico en la red, al brindar una plataforma para el filtrado y análisis de los datos generados por los sensores, utilizando recursos de los dispositivos que están en el propio borde de la red (*edge*). Como se ha mencionado anteriormente, una característica inherente a la computación en la niebla es la reducción de la latencia, especialmente útil para aplicaciones que requieren procesamiento en tiempo real. En (Hu et al, 2017) se ofrecen otras ventajas de este paradigma en relación con la sensibilidad a la ubicación, la distribución geográfica, el bajo consumo de energía, y la seguridad y protección de la privacidad. La computación en la niebla soporta las demandas de la movilidad basada en la ubicación y facilita a los administradores el control de dónde los usuarios y dispositivos móviles se encuentran y cómo acceden a la información.

Tales ventajas hacen particularmente apropiado el paradigma de computación en la niebla o *fog computing* para la gestión de datos provenientes de IoT, con mayor pertinencia en aquellas aplicaciones que no requieran un uso intensivo de recursos de procesamiento y/o almacenamiento, en cuyo caso la nube sigue siendo la más adecuada.

Tipos de aplicaciones beneficiarias de *fog computing*

De acuerdo a (Baktyan & Zahary, 2018) y considerando las ventajas discutidas, un enfoque de *fog computing* podría beneficiar a los tipos de aplicación siguientes:

- Aplicaciones que tienen requerimientos estrictos de latencia, tales como juegos de móviles, videoconferencia, etc.

- Aplicaciones geo-distribuidas donde los datos tienen una dispersión geográfica en amplias áreas, como monitoreo ambiental, estudios epidemiológicos u otras aplicaciones con análisis espacio-temporales.

- Aplicaciones móviles que requieren respuestas en tiempo cercano al real, conectadas a usuarios móviles, como vehículos conectados, control de flotas de transporte, etc.

- Grandes sistemas de control distribuido que utilizan un gran número de sensores y actuadores, como, por ejemplo, los sistemas inteligentes de luces de tráfico.

Algunos desafíos asociados al paradigma de *fog computing*

A pesar de múltiples y crecientes aplicaciones implementadas con *edge-fog computing*, este paradig-

Tabla 2. Desafíos tecnológicos de fog computing.

Dominio tecnológico	Desafío de la combinación IoT-Fog-Cloud
Fog y 5G	Mecanismos eficientes para incrementar redes complejas y heterogéneas que adopten diversas tecnologías (ej. LoRAWAN, Sixfox, NB-IoT) y que comprendan múltiples modelos de recursos de redes desde los dispositivos IoT, el borde, la niebla y la nube
Orquestación de servicios	Proveer múltiples niveles de analíticas de datos en tiempo real junto con eficientes mecanismos de optimización, considerando la gran cantidad de datos multidimensionales en escenarios IoT basados en fog computing. Desarrollo de mecanismos de seguridad que prevengan ataques de software, hardware y de red en los nodos fog, considerando su naturaleza dinámica, distribuida y de gran escala. También debe velarse por la privacidad de los datos, que pudiera ser potencialmente violada por la cercanía de los nodos fog al usuario IoT que genera los datos Implementar la orquestación de servicios en el entorno del llamado "network slicing" de 5G.
Gestión de microservicios	Reconfiguración de servicios que consideren requerimientos de calidad del servicio (QoS) para lograr la adaptación automática y transparente de la ejecución de microservicios.
Asignación y optimización de recursos	Sistemas de gestión de recursos y esquemas de planificación multi-criterio que puedan optimizar rápidamente la asignación de recursos para enfrentar la naturaleza dinámica de del sistema IoT-Fog-Cloud.
Consumo de energía	Gestión "económica" de datos, que implica una evaluación detallada de cuán frecuentemente puede ser necesario generar, transferir, almacenar o procesar todos los diferentes tipos de datos que se mueven en el ecosistema IoT-Fog-Cloud
Gestión de datos y ubicación	Medir y cuantificar el compromiso entre la ubicación de los datos y servicios en los niveles fog o cloud. Cómo seleccionar los servicios que van a ser localizados en los nodos edge-fog y por cuánto tiempo constituye un reto atendiendo a los múltiples factores que lo condicionan
Modelos de servicios y negocios	Mientras los modelos de servicio y negocio en la nube están muy bien establecidos, no está claro que las capas fog-edge puedan heredar tales modelos de forma idéntica. Es un desafío determinar cómo los servicios de IoT combinados con los de fog y cloud se ofrecen, monitorean y eventualmente se cobran, en un contexto heterogéneo de actores e intereses.

ma está aún en su infancia, por lo que existe un grupo de desafíos que marcarán investigaciones futuras en dicho campo. Existen desafíos de *fog computing* asociados tanto a dominios de aplicación, como a dominios tecnológicos. Para los dominios de aplicación, su empleo en entornos urbanos y en el contexto de Internet de las Cosas Industrial exhiben un conjunto de retos que han sido descritos en estudios recientes (Bittencourt, et al., 2018).

En cuanto a los desafíos tecnológicos, la tabla 2 resume un grupo de ellos, clasificados por dominio, que han sido extraídos de prominentes fuentes de los últimos 3 años (Bittencourt, et al., 2018), (Leoni-Santos, y otros, 2019), (von Leon, y otros, 2019).

Conclusiones

La computación en la niebla complementa al paradigma de computación en la nube, para reducir la latencia y el tráfico en la red ante la enorme generación de datos proveniente de la Internet de las Cosas, permitiendo, a su vez, un ahorro del ancho de banda y de energía. Gracias a su proximidad al borde de la red, este enfoque es sensible al contexto y a la distribución geográfica de los dispositivos; características que junto a su capacidad de hacerlos interoperar entre sí y de interactuar con la nube, les confiere a este paradigma un rol decisivo en la gestión de datos de IoT.

En este artículo se ofrece un bosquejo conceptual del paradigma *fog computing* para develar sus características, ventajas, principales aplicaciones y desafíos asociados.

Reaccionando a algunos de tales desafíos, un equipo mixto de la Unión de Informáticos de Cuba y la Universidad Tecnológica de La Habana “José Antonio Echeverría” se encuentra evaluando la plataforma de código abierto y gratuita FIWARE, sobre la cual se experimentarán escenarios mayormente enfocados a gestión de datos y orquestación de servicios basados en *fog computing*.

Paralelamente, se colabora en el marco del Grupo ANGeoSC de la Universidad Nacional de Colombia, en la generación de pruebas de concepto para potenciar el rol de las redes definidas por software (SDN), con el fin de soportar la interoperabilidad entre los dispositivos IoT que están en el borde de la red, los nodos niebla y la nube.

Referencias

Baktyan, A. A., & Zahary, A. T. (2018). A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. *EAI Endorsed Transactions on Internet of Things, 4*(14).

Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., Ranaf, O. (2018). The Internet of Things, Fog and Cloud Continuum: Integration and Challenges. 134-155. doi:arXiv:1809.09972v1 [cs.DC] 26 Sep 2018

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *MCC workshop on Mobile cloud computing.* ACM.

Buyya, R., & Narayana-Srirama, S. (2019). *Fog and Edge Computing: Principles and Paradigms.* New Jersey: John Wiley & Sons, Inc.

Heck, M., Edinger, J., Schäfer, D., & Becker, C. (2018). IoT Applications in Fog and Edge Computing: Where Are We and Where Are We Going? *27th International Conference on Computer Communication and Networks (ICCCN)* (págs. 1-6). IEEE.

IEEE Standards Association. (2018). *IEEE 1934-2018: IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing.* https://standards.ieee.org/standard/1934-2018.html.

Leoni-Santos, G., Ferreira, M., Ferreira, L., Kelner, J., Sadok, D., Albuquerque, E., . Takako-Endo, P. (2019). Integrating IoT + Fog + Cloud Infrastructures: System Modeling and Research Challenges. En R. Buyya, & S. Narayana-Srirama, *Fog and Edge Computing: Principles and Paradigms* (págs. 51-78). John Wiley & Sons, Inc.

Mahmud, R., Koch, F. L., & Buyya, R. (2018). Cloud-Fog Interoperability in IoT-enabled Healthcare Solutions. *ICDCN '18, 19th International Conference on Distributed Computing and Networking, January 4-7,2018* (pág. 10 pages). Varanasi, India: ACM.

Tárano, S., Delgado, T., & Pérez, A. (2018). Towards Smarter Cities Taking Advantage of the Fog Computing Paradigm. *Sistemas & Telemática*, 16(45), 19-30. 16(45) Doi:10.18046/syt.v16i45.275.

von Leon, D., Miori, L., Sanin, J., Ioini, N. E., Helmer, S., & Pahl, C. (2019). A Lightweight Container Middleware for Edge Cloud Architectures. En R. Buyya, & S. N. Srirama, *Fog and Edge Computing: Principles and Paradigms* (págs. 145-170). NJ: John Wiley & Sons, Inc.

Tatiana Delgado Fernández. *Es vicepresidenta de la Unión de Informáticos de Cuba y profesora del Departamento Informática Empresarial en la Universidad Tecnológica de La Habana. Graduada de Ingeniería en Sistemas Automatizados de Dirección (1989), tiene una maestría en Optimización y Toma de Decisiones (1997) y un doctorado en Ciencias Técnicas (2005). Dirige la revista cubana de Transformación Digital. Coordina y participa en varias investigaciones relacionadas con Internet de las Cosas, Big Data, Web Semántica y Transformación Digital.*

Computación en la niebla: conceptualización y aplicaciones

DOI: 10.29236/sistemas.n156a8

Resumen
El concepto de computación en la niebla es quizá tan difuso como el fenómeno meteorológico que representa, y es que cuando se trata de acercar de manera física la capacidad de almacenamiento, computación y comunicación de la nube a los billones de dispositivos que hoy componen internet de las cosas, son múltiples los caminos y las aproximaciones posibles. Por lo tanto, con el fin de aplicar el concepto adecuado en el contexto adecuado, el presente artículo pretende presentar y diferenciar los distintos conceptos relacionados con computación en la nube y en el borde, así como ofrecer claridad en sus dominios de aplicación, los cuales tienen en común el aprovechamiento de la localidad para optimizar tiempos de respuesta, mejorar la privacidad de los datos, ampliar la capacidad de personalización de los servicios y reducir el consumo de los recursos de red mediante el filtrado o tratamiento local de los datos.

Palabras claves
Computación en la niebla, computación en el borde, computación móvil, Internet de las Cosas (IoT), aplicaciones.

Introducción

En la era de la información, los datos son el bien más preciado por las organizaciones como el combustible que alimenta sus estrategias de direccionamiento basado en datos, por lo tanto, no es de sorprender que cuando se afirma que para el año en curso la cantidad de dispositivos en Internet de las Cosas (IoT) será de 50 mil millones, es decir, un promedio de 7 dispositivos por humano (McAfee & Brynjolfsson, 2012), se genere un amplio interés por los detalles técnicos y de arquitectura para la correcta explotación de los datos producidos. Este fenómeno se contrasta con la creciente adopción de la nube para procesos analíticos (Rai, Sahoo, & Mehfuz, 2015), pues es la nube la tecnología preferida a la hora de tratar gran cantidad de datos dadas sus capacidades virtualmente ilimitadas de almacenamiento, procesamiento y comunicación. Esta convergencia de fenómenos descrita, ha llevado a que la nube sea el lugar natural para realizar el procesamiento de los datos producidos por IoT (Yousefpour, y otros, 2019).

Sin embargo, utilizar las bondades de las nubes públicas implica la transmisión de datos a través de varios dispositivos de comunicación a centros de datos potencialmente distantes, lo que no es permisible para algunas aplicaciones IoT críticas que necesitan tiempos de respuesta inmediatos, sensibles a la ubicación o con dispositivos en ubicaciones remotas con comunicación intermitente. Por lo tanto, se hace necesario acercar físicamente las capacidades de la nube a los dispositivos IoT, lo que permitiría superar los retos anteriormente descritos, pero además, ampliar la cantidad de datos centralizados en la nube, pues en la actualidad alrededor del 20% es almacenado en la nube y únicamente el 5% de ellos es procesado para generar valor (Salem & Nadeem, 2016).

Ante el reto de acercar la nube a los dispositivos IoT, son múltiples las alternativas propuestas, los autores en (Yousefpour, y otros, 2019) hacen un recorrido extensivo de cada una de ellas, desde las más extremas que llevan la computación y almacenamiento a los dispositivos mismos como la computación en la bruma hasta las más sofisticadas como los *cloudlet*. De cualquier forma, la lista dista de ser exhaustiva y el lector podrá tener casos de aplicación en donde sea necesaria una combinación de aproximaciones o incluso una aproximación totalmente nueva, por lo tanto, se presentan también los pilares de arquitectura definidos por el consorcio *OpenFog* como una guía para la reproducción de buenas prácticas en toda arquitectura de computación en el borde o en la niebla.

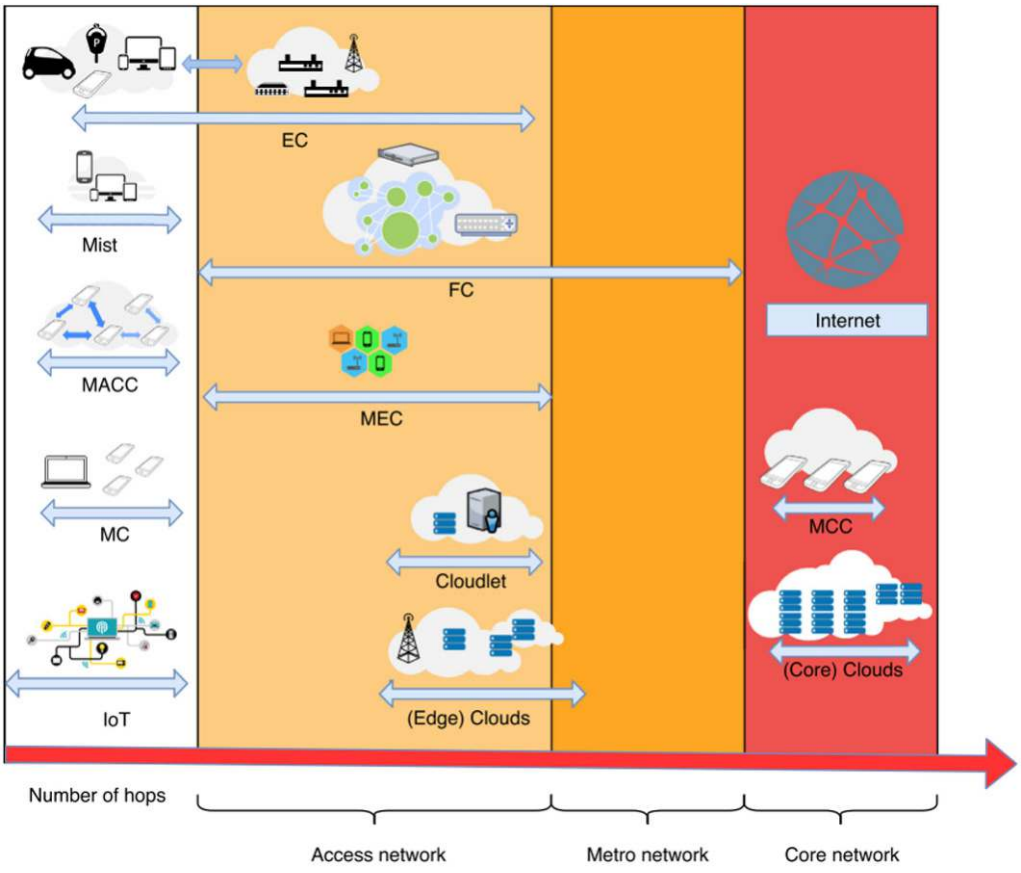
Así pues, el presente artículo inicia con la definición de los conceptos asociados, seguido de los pilares de arquitectura para cualquier solución de computación en el borde o en la niebla, seguido de una presentación de dominios de aplicación idóneos o en los que ya se aplica el paradigma y termina con conclusiones y discusiones finales.

Conceptualización

La computación en la niebla extiende el paradigma de la computación en la nube a las redes de comunicación cercanas a los dispositivos IoT, esto permite contar con características adicionales como: baja latencia y sensibilidad a la ubicación, distribución geográfica expandida, movilidad, soporte a gran cantidad de dispositivos, comunicación inalámbrica predominante, soporte a aplicaciones en línea y heterogeneidad (Bonomi, Milito, Zhu, & Addepalli, 2012).

No obstante, cuando se trata de computación en la niebla no se cumple el precepto de "*one-size-*

Figura 1.



fits-all". Con esto presente, se describen a continuación algunas de las aproximaciones encontradas en la literatura desde la más próxima a la más lejana de los dispositivos IoT.

Figura 1. Comparación de la computación en la nube y sus paradigmas computacionales relacionados en términos de su ubicación y distancia a las nubes centrales (traducción propia) (Yousefpour, y otros, 2019, pág. 295).

- *Computación en la bruma* (*Mist Computing)*: Se trata de la forma más extrema de computación en el borde, pues se trata de usar los dispositivos IoT para realizar las tareas de computación y almacenamiento de datos. Por supuesto, esta aproximación tiene las limitaciones propias de los dispositivos y no es adecuada para el tratamiento de datos históricos o de grandes cantidades de datos (*big data)*, pero es una gran alternativa para aplicaciones que usan exclusivamente datos recientes (*hot data)* o que pueden usar resultados de procesamiento de capas de mayor capacidad como datos en caché.

- *Computación ad hoc móvil* (*Mobile Ad Hoc Computing – MACC)*: Se tratan de redes de comunicación que se generan de manera espontánea y temporal entre distintos dispositivos móviles y que permite generar clústeres descentralizados de comunicación, almacenamiento y cómputo. Este tipo de computación es altamente dinámica y tiene aplicación en contextos colaborativos como ayudas en desastres naturales, emisión de videos grupales o sistemas vehiculares colaborativos (ej. Flotas de drones).

- *Computación móvil* (*Mobile Computing – MC)*: Se trata de un subconjunto de la computación en la bruma, en el cual los dispositivos son únicamente móviles e.j. celulares, tabletas o laptops y que merece su categoría aparte, pues estos dispositivos pueden tomar ventaja de las redes móviles y los servicios de ubicación con los que cuentan, para crear aplicaciones sensibles al contexto tales como recordatorios basados en la ubicación (Yousefpour, y otros, 2019).

- *La nube de las cosas* (*Cloud of Things)*: En la misma línea de la computación en la bruma, la nube de las cosas propone agregar una capa de virtualización a los recursos computacionales en el borde con el fin de ofrecer servicios de comunicación, almacenamiento y computación similares a la nube. Teniendo en cuenta la gran cantidad de dispositivos en el borde y la creciente capacidad de computo con la que cuentan, esta aproximación promete ser una solución para una

amplia gama de aplicaciones críticas de IoT. Sin embargo, tiene retos en términos de privacidad de los datos y motivación de los dispositivos para participar.

- *Computación en el borde* (*Edge computing)*: Se trata de la computación que se lleva a cabo en la red local de los dispositivos IoT. Es decir, permite agregar nodos computacionales distintos a los dispositivos IoT, siempre y cuando los mismos se encuentren a máximo un dispositivo de comunicación (*hop*) de los mismos. En estas capas es común encontrar dispositivos como las tarjetas *Raspberry pi* que permiten la ejecución de código C++/Python de manera eficiente permitiendo la ejecución de servicios de coordinación y/o procesamiento.

- *Computación en la niebla* (*Fog Computing)*: El paradigma de la computación en la niebla pretende cerrar la brecha existente entre la computación en la nube y los dispositivos IoT, mediante la generación de servicios intermedios que permitan por un lado responder a tiempo para las aplicaciones críticas de IoT y por otro lado, filtrar y comprimir la cantidad de datos que llegan a la nube para ganar eficiencias tanto en costos como en procesamiento. La visión de la computación en la niebla es que las funciones de comunicación, almacenamiento, procesamiento y aceleración tan avanzadas en la nube, puedan ser parte de un flujo continuo nube a dispositivo (*cloud to thing continuum)* aprovechando las ventajas de cada una de las capas de comunicación y con consideraciones de latencia y localidad.

- *Computación móvil en el borde* (*Mobile Edge Computing – MEC)*: Así como la computación en la bruma se extiende a la red de acceso con la computación en el borde, la computación móvil se extiende a la red de acceso con la computación móvil en el borde, permitiendo la integración de mayor cantidad de dispositivos móviles. Un ejemplo de configuración de redes que permite este tipo de computación son las redes locales inalámbricas (WLAN).

- *Cloudlets*: Se tratan de pequeños centros de datos ubicados en la red de acceso de los dispositivos móviles que permiten disminuir la carga de los dispositivos IoT mediante la generación de servicios de computación usando técnicas de virtualización. Dado que se pueden establecer relaciones de confianza entre los dispositivos IoT y los *cloudlet*, este paradigma encuentra amplia aplicación en situaciones en donde la privacidad y seguridad de los datos es una preocupación mayor, además al tratarse de recursos vir-

tualizados, pueden ser fácilmente llevados a la nube en caso de necesitar mayor escala.

- *Nube en el borde*: En la actualidad las nubes públicas *Amazon Web Services* (AWS) y Azure ofrecen servicios para la instalación de capacidades de almacenamiento y procesamiento de sus respectivas nubes en el borde, mediante el envío de dispositivos computacionales con algunos de sus servicios preinstalados y configurados. En el caso de AWS, la oferta recibe el nombre de *Snowball Edge*[1] y en el caso de *Azure*, *Azure Stack*[2].

- *Computación en la nube*: Ofrece servicios de comunicación, almacenamiento, procesamiento como servicio a distintos niveles: infraestructura, plataforma y software. La computación en la nube se basa en múltiples centros de datos geográficamente distribuidos alrededor del mundo con capacidades tan amplias que para efectos prácticos son consideradas ilimitadas. Los casos de uso que soporta la computación en la nube son mucho más amplios que IoT, sin embargo, los principales proveedores han entendido la importancia y crecimiento exponencial de este ámbito y han creado servicios para soportar el desarrollo de aplicaciones IoT por ejemplo: AWS IoT[3], Azure IoT[4] y GCP IoT[5].

Pilares de arquitectura

De acuerdo con el consorcio *OpenFog* estos son los pilares sobre los que se debería construir cualquier arquitectura que acerque la computación, almacenamiento, comunicación, control y aceleración a los dispositivos IoT (OpenFogConsortium, 2017):

- Seguridad: Se debe garantizar la cadena de confianza entre los nodos, así como la privacidad de los datos y la fiabilidad de los canales de comunicación.

- Escalabilidad: La niebla debe poder escalar tanto vertical como horizontalmente, esto con el fin de soportar nodos con cargas desbalanceadas bien sea adyacentes o en capas adyacentes. Así mismo, se deben poder agregar o eliminar nodos de la red de manera flexible y de acuerdo con la carga actual.

- Naturaleza Abierta: La computación en la niebla debe ser descentralizada e interoperable sin parcialidades hacia algún proveedor de software o hardware específico, esto con el fin de permitir la integración de cualquier tipo de nodo en cualquier tipo de red.

- Autonomía: Los nodos de la niebla deben poder seguir prestan-

[1] https://aws.amazon.com/es/snowball/
[2] https://azure.microsoft.com/es-es/overview/azure-stack/
[3] https://aws.amazon.com/es/iot/
[4] https://azure.microsoft.com/es-es/overview/iot/
[5] https://cloud.google.com/solutions/iot?hl=es

do servicio incluso ante fallas en capas superiores de jerarquía, es decir que debe existir inteligencia local y autonomía en las redes locales de nodos para poder tomar decisiones ante situaciones extremas.

- Robustez, Alta Disponibilidad y Servicio Continuo: Los servicios ofrecidos deben tener consideraciones de robustez, alta disponibilidad y servicio continuo, en especial teniendo en cuenta las condiciones desafiantes que pueden tener algunas capas de la jerarquía con dispositivos en ubicaciones remotas con comunicación limitada. La principal consideración en este pilar es la dispensabilidad de todos los nodos de la red como principio básico de diseño y el uso de la nube como lugar de almacenamiento de copias de apoyo e históricos.

- Agilidad: Este pilar hace referencia a la capacidad de la red de nodos de tomar decisiones operacionales sin la intervención humana, lo anterior data la imposibilidad humana de analizar toda la información producida y la necesidad de decisiones ágiles. Además, este pilar hace referencia a la capacidad de adaptación frente a la dinámica de cambio de la niebla.

- Programabilidad: Así como se soporta la programación tanto a nivel del procesamiento de los datos o los servicios ofrecidos, como a nivel de infraestructura. Es decir, se debe soportar el paradigma de infraestructura como código.

- Jerarquía: A pesar de no ser esencial para una arquitectura en la niebla, se expresa en la mayoría de los despliegues, pues cada una de las capas que de los dispositivos llevan a la nube tienen requerimientos y características diferenciadas lo que hace que sea necesario no solo coordinación sino jerarquía entre los despliegues de la niebla en cada una de estas capas. Por ejemplo, una gran organización puede contar con inteligencia local en cada una de sus sedes, no obstante, la evolución y monitoreo de esa inteligencia se monitorea desde la sede central.

Aplicaciones

Son numerosas las industrias que hoy en día están tomando ventaja de la computación en el borde y en la niebla, a continuación, algunos ejemplos encontrados en la literatura:

- Agricultura inteligente (Galvão, y otros, 2019): monitoreo de cultivos a través de múltiples sensores.

- Transporte Inteligente (Galvão, y otros, 2019): monitoreo de flotas de buses para mejorar agendamiento de salidas y proveer de

servicios inteligentes a los usuarios.

- Salud y bienestar inteligente (Galvão, y otros, 2019) (Preden, y otros, 2015): uso inteligente de datos producidos por dispositivos *wearable* de usuarios de parques públicos para mejorar infraestructura.

- Recolección de desechos inteligente (Galvão, y otros, 2019): despliegue de dispositivos inteligentes a nivel metropolitano para medir niveles de contenedores y planear inteligentemente rutas de camiones recolectores

- Redes eléctricas inteligentes (Galvão, y otros, 2019): Dominio con necesidad de respuesta inmediatas y colaboración entre los distintos nodos, propicio para despliegues en la niebla.

- *Retail* inteligente (Galvão, y otros, 2019): Dominio de aplicación con necesidades jerárquicas de respuesta, en donde la operación, inventario y publicidad necesitan respuestas inmediatas, pero el direccionamiento basado en inteligencia de negocios evoluciona a menor ritmo y con necesidades de procesamiento de gran cantidad de datos.

- Parqueo Inteligente (Grassi, Bahl, Jamieson, & Pau, 2017): Tratamiento de imágenes producidas en vehículos inteligentes de manera colaborativa para el mapeo de espacios libres de parqueo en una ciudad.

- Vehículos Conectados (Bonomi, Milito, Zhu, & Addepalli, 2012): Redes *ad hoc* de vehículos formados por cercanía que colaboran entre sí para mayor seguridad en la vía.

Conclusiones

Con un estimado de 7 dispositivos interconectados por cada ser humano que habita la tierra y el alto dinamismo del mundo actual que exige información con sentido, en tiempo real, y extraída de una inmensa cantidad de datos que deben ser interpretados en un contexto particular, la computación en la niebla se perfila como una alternativa que permite reducir los tiempos de comunicación y tomar ventaja de la colaboración para producir un *cloud to thing continuum* que permita acercar las bondades de la nube a los dispositivos. Sin embargo, como lo evidencia el presente artículo, son diversas las alternativas que se han propuesto para la computación en la niebla y en el borde, por lo que es importante reconocerlas y poder discernir el caso de aplicación específico, para el cual se adapta cada una.

Referencias

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop, 13-15.

Galvão, J., Sousa, J., Machado, J., Mendonça, J., Machado, T., & Silva, P. (2019). Mechanical design in industry 4.0: Development of a handling system using a modular approach. Lecture Notes in Electrical Engineering, 505(3), 508-514.

Grassi, G., Bahl, P., Jamieson, K., & Pau, G. (2017). ParkMaster: An in-vehicle, edge-based video analytics service for detecting open parking spaces in urban environments. 2017 2nd ACM/IEEE Symposium on Edge Computing, SEC 2017.

McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. Harvard business review, 90, 60-66, 68, 128.

OpenFogConsortium. (Febrero de 2017). Obtenido de Open Fog Consortium: https://www.openfogconsortium.org/ra/

Preden, J., Tammemae, K., Jantsch, A., Leier, M., Riid, A., & Calis, E. (2015). The Benefits of Self-Awareness and Attention in Fog and Mist Computing. Computer, 48(7), 37-45.

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. SpringerPlus, 4(1), 1-12.

Salem, A., & Nadeem, T. (2016). LAMEN: Leveraging resources on anonymous mobile edge nodes. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, 03-07-Octo, 15-17.

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., . . . Jue, J. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture, 98(February), 289-330.

Andrés Felipe Cantor Albarracín. *Ingeniero de Sistemas y Magíster en Ingeniería de Sistemas y Computación de la Universidad Nacional de Colombia, cuenta con más de cinco años de experiencia en la implementación de soluciones Big Data y analítica para organizaciones que han decidido tomar estrategias dirigidas por los datos. Su investigación se centra en Internet de las Cosas y semántica para la interoperabilidad.*

22
AL
26
SEP

TACTICAL EDGE LATAM VIRTUAL SUMMIT

Uno de los mejores eventos de ciberseguridad de América Latina

HTTPS://TACTICALEDGE.CO